Ατομική Διπλωματική Εργασία

Το πρόβλημα του εξαναγκασμού
στα διαδικτυακά εκλογικά συστήματα

Γιώργος Κουμέττου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2014

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ ΕΞΑΝΑΓΚΑΣΜΟΥ ΣΤΑ ΔΙΑΔΙΚΤΥΑΚΑ ΕΚΛΟΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

Κουμέττου Γιώργος

Επιβλέπουσα Καθηγήτρια
Δρ. Άννα Φιλίππου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2014

Ευχαριστίες

Πρώτα απ'όλα, είμαι ευγνώμων στους γονείς μου Κουμέττο και Ιωάννα Κουμέττου, για την ολόψυχη αγάπη και υποστήριξη τους αυτά τα χρόνια. Αφιερώνω αυτή την εργασία στον πατέρα μου και στην μητέρα μου. Θα ήθελα να εκφράσω τις ειλικρινές μου ευχαριστίες στην επιβλέπουσα καθηγήτρια μου, κυρία Άννα Φιλίππου για την πολύτιμη βοήθεια και καθοδήγηση της κατά την διάρκεια της δουλειάς μου.

Περίληψη

Η παρούσα ΑΔΕ ασχολείται, με τα συστήματα εκλογών μέσω διαδικτύου. Εξετάζει και παρουσιάζει την μελέτη γύρω από το πρόβλημα του εξαναγκασμού (coercion) στις εξ αποστάσεως ψηφοφορίες. Παρουσιάζεται το πρόβλημα του εξαναγκασμού, και το σύστημα Civitas. Γίνεται μια εκτενής περιγραφή του συστήματος και των βελτιώσεων που προτάθηκαν. Έμφαση δίνεται στην διαδικασία της εγγραφής και στα προβλήματα που παρουσιάζει μια εξ αποστάσεως εγγραφή.

Επιπλέον παρουσιάζεται η έννοια της επαληθευσιμότητας των αποτελεσμάτων και πως αυτή δυσχεραίνεται με το πρόβλημα της αντίστασης στον εξαναγκασμό.

Τέλος παρουσιάζεται ένα σύστημα ψηφοφορίας μέσω διαδυκτίου που αντιμετωπίζει το πρόβλημα του εξαναγκασμού. Πρόκειται για διαδικτυακή εφαρμογή δημιουργημένη με Django , twitter Bootstrap, jQuery, CSS και HTML.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Κίνητρο

Οι ψηφοφορίες αποτελούν βασική παράμετρο δημοκρατίας . Δια μέσου των αιώνων οι διαδικασίες και τεχνικές που χρησιμοποιούνταν, άλλαζαν και βελτιώνονταν,πάντα με στόχο τις πιο δίκαιες εκλογικές αναμετρήσεις.

Σήμερα, που το διαδίκτυο έχει μπει για τα καλά στις ζωές ενός πολύ μεγάλου ποσοστού του πληθυσμού, πολύ αβίαστα προκύπτει η εξής ερώτηση:

“Αφού μπορώ να εμπιστευτώ τις συναλλαγές , και τα χρήματα μου στο διαδίκτυο, γιατί να μην μπορώ να εμπιστευτώ την ψήφο μου;”

Η παρούσα διπλωματική εργασία σκοπό έχει να προσεγγίσει την πιο πάνω ερώτηση παρουσιάζοντας τις παραμέτρους ασφαλείας, οι οποίες κάνουν πολλούς ερευνητές να προβληματίζονται [1] [2] [3] [4], για το αν οι εκλογές μέσω διαδικτύου, μπορούν όντως να υιοθετηθούν. Επιπλέον επικεντρώνεται στο πρόβλημα του εξαναγκασμού (coercion), παρουσιάζοντας την μέχρι τώρα δουλειά που έχει γίνει προς επίλυση του συγκεκριμένου προβλήματος.

Η ψηφοφορία , μέσω διαδικτύου, επιτρέπει στους χρήστες να ψηφίζουν από το σπίτι τους, ή από όπου άλλου επιθυμούν. Αυτό σημαίνει πως ανεξαρτήτου γεωγραφικής θέσης και συνθηκών, κάθε

πολίτης που είναι εγγεγραμμένος στους εκλογικούς καταλόγους, μπορεί να ψηφίσει , φτάνει να έχει στην κατοχή του υπολογιστή με πρόσβαση στο διαδίκτυο. Επιπλέον αφού οι εκλογές γίνονται ηλεκτρονικά, τα αποτελέσματα των εκλογών μπορούν να υπολογίζονται και ανακοινώνονται πολύ πιο σύντομα. Το χρονικό αλλά και χρηματικό κόστος των εκλογών μπορεί να μειωθεί δραματικά, γεγονός που μπορεί να δώσει το έναυσμα για υιοθέτηση πολιτικών άμεσης δημοκρατίας, δηλαδή συχνότερα ηλεκτρονικά δημοψηφίσματα, με χαμηλό κόστος, ώστε να εκφράζεται η θέληση του λαού για σημαντικά εθνικά ζητήματα.

Για να είναι εφικτή η εκμετάλλευση των προτερημάτων των εκλογών μέσω διαδικτύου, είναι αναγκαίος ο σχεδιασμός ενός ασφαλούς και έμπιστου συστήματος.

1.2 Στόχοι Διπλωματικής Εργασίας

Η Διπλωματική αυτή εργασία, έχει ως ένα από τους στόχους της να μελετήσει το πρόβλημα του εξαναγκασμού στις διαδικτυακές ψηφοφορίες. Πρόβλημα εξαναγκασμού σε διαδικτυακές εκλογικές αναμετρήσεις , υπάρχει εφόσον ο κάθε ψηφοφόρος μπορεί να ψηφίζει από όπου θέλει και έτσι όποιοσδήποτε είναι κοντά του κατά την στιγμή της ψηφοφορίας, μπορεί να δει τι και πως ψηφίζει . Κάτι τέτοιο παραβιάζει την μυστικότητα της ψήφου. Άρα για χάρη χρημάτων ή υπό τις απειλές κάποιων, ενδέχεται να ψηφίσει με συγκεκριμένο τρόπο, αφού ο τρόπος με τον οποίο ψήφισε μπορεί εύκολα να διαρρεύσει. Έτσι υφίσταται η αγορά ψήφων, που θέλουμε να αποφύγουμε.

Παράλληλα ομως υπάρχει το ζήτημα της επαληθευσιμότητα των αποτελεσμάτων. Δηλαδή κάθε εξωτερικός παρατηρητής πρέπει να είναι σε θέση να επαληθεύσει τα αποτελέσματα, χωρίς ομως το σύστημα να διαρρέει όποιαδήποτε πληροφορία για το πως ψήφισαν οι χρήστες. Η επαληθευσιμότητα των αποτελεσμάτων όμως είναι δύσκολο να υπάρξει χωρίς την παραβίαση της απαίτησης που υπάρχει για αντιμετόπιση του προβλήματος εξαναγκασμού. Πρόκειται για αντικρουόμενες απαιτήσεις, και μέσα στους στόχους της εργασίας είναι να εξεταστεί αν και σε πιο βαθμό αυτές οι δύο ιδιότητες μπορούν να ικανοποιούνται ταυτόχρονα.

Τέλος ακόμη ένας στόχος είναι η υλοποίηση ενός συστήματος ηλεκτρονικής ψηφοφορίας με έμφαση στην κάλυψη της ιδιότητας του εξαναγκασμού, και να εξετάσει αν και πως μπορεί να προστεθεί σε αυτό η απαίτηση για επαληθευσιμότητα των αποτελεσμάτων.

1.3 Δομή Εργασίας

Στο δεύτερο κεφάλαιο παρουσιάζονται οι απαιτήσεις που υπάρχουν σε συστήματα ψηφοφορίας. Συγκεκριμένα γίνεται αναφορά στις βασικές απαιτήσεις : ακεραιότητα, μυστικότητα ψήφου, ταυτοποίηση ψηφοφόρου και διαθεσημότητα.

Στο τρίτο κεφάλαιο παρουσιάζεται το σύστημα κρυπτογράφησης ElGamal το οποίο χρησιμοποιείται για των διαμοιρασμό των μυστικών κλειδιών μεταξύ δύο οντοτήτων. Ακολούθως γίνεται αναφορά στα πρωτόκολλα μηδενικής γνώσης, χρήσιμα στα συστήματα ψηφοφορίας που υποστηρίζουν επαληθευσιμότητα αποτελεσμάτων, ώστε να επιτρέπουν επαλήθευση χωρίς να αποκαλύπτεται κάποια πληροφορία για τον τρόπο με τον οποίο κάποιος ψηφοφόρος ψήφισε. Επιπλέον γίνεται αναφορά στον πρόβλημα του διαμοιρασμού μυστικού μηνύματος, κατά το οποίο απαιτείται συγκεκριμένος αριθμός οντοτήτων ώστε να αποκαλυφθεί το μυστικό, που στην περίπτωση του συστήματος Civitas που θα μελετηθεί, αφορά τον διαμοιρασμό των κλειδιών από κάθε υπεύθυνο εγγραφής στους ψηφοφόρους, κατα τρόπο που έστω και ένας μόνο υπεύθυνος να είναι έμπιστος, το συνθηματικό δεν θα μπορεί να διαρρεύσει. Στο τέλος του δεύτερου κεφαλαίου, γίνεται αναφορά στα δίκτυα μήξης, που χρησιμοποιούνται τόσο στην δημιουργία ανώνυμων καναλιών , όσο και ως μέθοδος απόδειξης μηδενικής γνώσης για επαλήθευση των αποτελεσματων.

Στο τέταρτο κεφάλαιο παρουσιάζεται το πρόβλημα του εξαναγκασμού, και το σύστημα Civitas. Παρουσιάζονται οι δυνατότητες του επιτιθέμενου που δίνονται σε αυτό το σύστημα, οι κατηγορίες ατόμων που το αποτελούν και οι φάσεις λειτουργίας του. Παρουσιάζεται η κεντρική ιδέα για αντιμετώπιση του εξαναγκασμού, και ακολούθως αναλύονται οι φάσεις λειτουργίας του, με ιδιαίτερη έμφαση να δίνεται στην διαδικασία της εγγραφής. Ακολούθως παρουσιάζεται η απαίτηση της επαληθευσιμότητας των αποτελεσμάτων. Έχοντας εξηγήσει τον τρόπο με τον οποίο είναι εφικτή η επαλήθευση των αποτελεσμάτων, εξηγείται γιατί είναι δύσκολο να υπάρχει ταυτόχρονα μηχανισμός για άμυνα έναντι του εξαναγκασμού και μηχανισμός για επαλήθευσης των αποτελεσμάτων.

Στο πέμπτο κεφάλαιο παρουσιάζονται οι απαιτήσεις χρήσης του εκλογικού συστήματος που υλοποιήθηκε στα πλαίσια της διπλωματικής εργασίας, και ακολούθως επεξηγείται ο τρόπος

λειτουργίας του , ξεκινώντας από την παρουσίαση της βάσης δεδομένων και ακολούθως επεξηγείται αναλυτικά η κάθε φάση του συστήματος.

Στο έκτο κεφάλαιο καταγράφονται τα συμπεράσματα που προέκυψαν μέσα από την μελέτη του συγκεκριμένου προβλήματος .

Κεφάλαιο 2

Ψηφοφορία μέσω διαδυκτίου

2.1 Απαιτήσεις εκλογικών συστημάτων

Για να είμαστε σε θέση να σχεδιάσουμε ένα “ασφαλές” και “έμπιστο” σύστημα, πρέπει πρώτα να καθορίσουμε τι εννοούμε με τους όρους ασφαλές και έμπιστο. Να καθοριστεί με σαφήνεια δηλαδή, πότε ένα σύστημα μπορεί να χαρακτηριστεί ως ασφαλές και έμπιστο, και άρα μπορεί να βοηθήσει στην διεξαγωγή έγκυρων εκλογικών αναμετρήσεων

Για να θεωρείται μια εκλογική αναμέτρηση έγκυρη, να είμαστε σίγουροι πως δεν υπήρξε αλλοίωση αποτελεσμάτων και κάθε ψήφος που μετρήθηκε αντικατόπτριζε πράγματι την θέληση του ψηφοφόρου, λαμβάνονται υπόψιν τα εξής:

Ακεραιότητα: Υπάρχει ακεραιότητα στην εκλογική αναμέτρηση, εάν κάθε ψήφος που είναι έγκυρη μετρήθηκε, και κάθε ψήφος που μετριέται αντιστοιχεί στην πραγματική πρόθεση ψήφου του χρήστη. Το ψηφοδέλτιο πρέπει να είναι προσεκτικά σχεδιασμένο ώστε ο ψηφοφόρος να είναι σε θέση να σημειώσει την επιλογή του με τον σωστό τρόπο στο ψηφοδέλτιο. Από την στιγμή της τοποθέτησης της ψήφου , μέχρι και μετά την καταμέτρηση της, το ψηφοδέλτιο δεν πρέπει να αλλοιωθεί. Κάθε ψήφος μετριέται όπως ακριβώς την σημείωσε ο ψηφοφόρος στο ψηφοδέλτιο.

Μυστικότητα ψήφου: Κάθε ψηφοφόρος πρέπει να έχει την δυνατότητα να κρατήσει κρυφή την ψήφο του. Επιπλέον όμως, ένα εκλογικό σύστημα πρέπει να διασφαλίζει πως όχι μόνο ο κάθε ψηφοφόρος θα μπορεί να κρατήσει μυστική την ψήφο του , αλλά και ότι, έστω και εάν θέλει να

αποδείξει σε έναν τρίτο πως ψήφισε με ένα συγκεκριμένο τρόπο δεν θα είναι σε θέση να το κάνει. Το δεύτερο χαρακτηριστικό , διασφαλίζει άμυνα έναντι επιθέσεων εξαναγκασμού, αφού ο ψηφοφόρος μη μπορώντας να αποδείξει πως/τι ψήφισε δεν θα μπορεί να πουλήσει την ψήφο του, ούτε να δεχθεί απειλές για το πως θα ψηφίσει.

Ταυτοποίηση ψηφοφόρων: Σε ένα σύστημα ψηφοφορίας πρέπει να διασφαλίζεται πως μόνο ψηφοφόροι εγγεγραμμένοι στους εκλογικούς καταλόγους μπορούν να ψηφίζουν , και επιπλέον πως για κάθε ψηφοφόρο μετριέται μία ψήφος.

Διαθεσιμότητα: Το σύστημα πρέπει να είναι λειτουργικό και διαθέσιμο κατά την διάρκεια όλης της ψηφοφορίας. Να είναι σε θέση να δίνει τα σωστά αποτελέσματα όταν ζητείται. Τέλος το σύστημα πρέπει να είναι διαθέσιμο σε κάθε εγκεκριμένο ψηφοφόρο, ώστε όλοι οι εγκεκριμένοι ψηφοφόροι να έχουν την δυνατότητα να ψηφίσουν. Αυτό το ζήτημα έχει τις ιδιαιτερότητες του όταν οι εκλογές γίνονται μέσω μέσω διαδικτύου (περίπτωση που πραγματεύεται η παρούσα διπλωματική εργασία), εξαιτίας της ύπαρξης επιθέσεων όπως DoS στο σύστημα.

Έτσι κάθε εκλογικό σύστημα είναι ασφαλές και έμπιστο , αν και μόνο αν οι προαναφερθείσες απαιτήσεις ικανοποιούνται . Κάποιες από τις προαναφερθέντες απαιτήσεις παρουσιάζουν συγκρούσεις μεταξύ τους εάν διασφαλιστούν με συγκεκριμένο τρόπο. Για παράδειγμα το σύστημα θα μπορούσε να κρατά τι ψήφισε ο κάθε ψηφοφόρος ώστε να εξασφαλίσει ότι υπάρχει ακεραιότητα και επαληθευσιμότητα. Αυτό όμως αμέσως θα παραβίαζε την απαίτηση για μυστικότητα ψήφου.

Στην παρούσα διπλωματική εργασία υπάρχει ιδιαίτερο ενδιαφέρον στην μυστικότητα ψήφου, αφού θα αναλυθούν συστήματα σχεδιασμένα ειδικά για να δώσουν λύση στο πρόβλημα εξαναγκασμού (coercion), που μπορεί να υπάρξει μόνο αν υπάρχει αδυναμία στην ικανοποίηση της απαίτησης μυστικότητας ψήφου. Ο Josef Benaloh, εχει δώσει τον εξής ορισμό [7]:

Receipt Freeness: Ένας ψηφοφόρος δεν πρέπει να είναι σε θέση να παράξει πληροφορία τέτοια που να μπορεί να πείσει οποιονδήποτε άλλον ότι ψήφισε με συγκεκριμένο τρόπο.

Πληρώντας αυτή την ιδιότητα κατά τον σχεδιασμό ενός συστήματος, είναι βέβαιο ότι αντιμετωπίζονται φαινόμενα αγοράς ψήφων και εξαναγκασμού των ψηφοφόρων να ψηφίσουν με

συγκεκριμένο τρόπο. Ένα τέτοιο σύστημα δεν μπορεί να είναι βέβαιο πως η ψήφος που καταχωρήθηκε προέρχεται από τον σωστό χρήστη, αφού ο ίδιος ο χρήστης μπορεί να άφησε κάποιον άλλο να ψηφίσει στην θέση του, ή να εξαναγκάστηκε να μην ψηφίσει καθόλου. Για αυτούς τους λόγους, οι Juels, Catalano and Jakobsson, δίνουν ένα πιο αυστηρό ορισμό της αντίστασης στον εξαναγκασμό (Coercion resistance), αφού πρώτα αναφέρουν τις δυνατότητες που έχει ο επιτιθέμενος .

Ο επιτιθέμενος μπορεί να απαιτήσει :

- να ψηφίσουν με ένα συγκεκριμένο τρόπο
- να αποκαλύψουν τα συνθηματικά τους
- να απέχουν από την εκλογική διαδικασία.

Έτσι ένα σύστημα εκλογών έχει αντοχή στον εξαναγκασμό (coercion-resistant) εάν είναι αδύνατο για τον επιτιθέμενο να γνωρίζει ότι ο ψηφοφόρος όντως ικανοποίησε τις δικές του απαιτήσεις.

Τα συστήματα που εξετάζονται σε επόμενη ενότητα θα αξιολογηθούν με βάση ακεραιότητα,μυστικότητα ψήφου,ταυτοποίηση ψηφοφόρων,διαθεσιμότητα, με ιδιαίτερη έμφαση να δύνεται στο πως τα συστήματα αυτά αντιμετωπίζουν το πρόβλημα εξαναγκασμού .

2.2 Σχετική εργασία

Σε αυτή την υπο-ενότητα γίνεται αναφορά στην μέχρι τώρα εργασία που έγινε προς επίλυση του προβλήματος εξαναγκασμού στις εκλογικές αναμετρήσεις

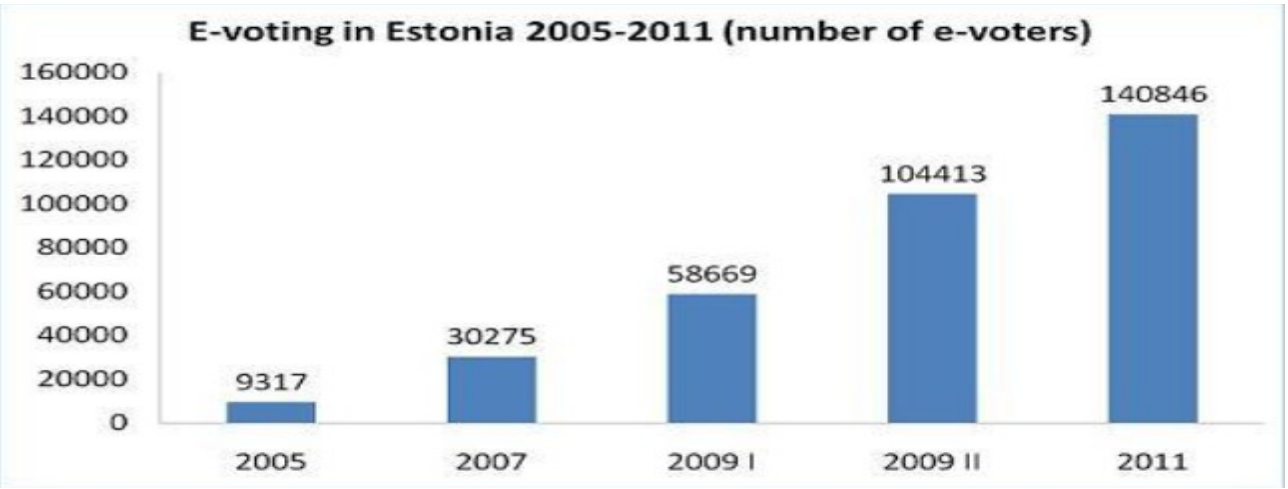
Σχετικά με τα πρωτόκολλα κρυπτογραφίας που χρησιμοποιούνται σε εξ αποστάσεως εκλογές μέσω διαδικτύου, οι Krishna Sampigethaya και Radha Poovendran, σε εργασία υπό τον τίτλο “A framework and taxonomy for comparison of electronic voting schemes” [9], παρουσιάζουν το έτος 2006 μια εκτενή σύγκριση των προτοκόλλων που υπήρχαν μέχρι την στιγμή εκείνη . Ο Martin Hirt στην εργασία του με τίτλο “Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting” [8], κάνει αναφορά και εξηγεί πως πρωτόκολλα βασισμένα σε mixnet, blind signatures και ομομορφική κρυπτογράφηση , λειτουργούν στα πλαίσια των πρωτοκόλλων κρυπτογραφίας που χρησιμοποιούνται για ψηφοφορίες μέσω διαδικτύου .

Ο Benaloh και ο Tuinstra [7] , παρατήρησαν πως όλα τα συστήματα ψηφοφορίας που υπήρχαν, έδιναν στον ψηφοφόρο μια ένδειξη , βάση της οποίας μπορούσαν να αποδείξουν ότι ψήφισαν με συγκεκριμένο τρόπο. Κάτι τέτοιο, όπως προαναφέρθηκε μπορεί να χρησιμοποιηθεί ώστε ο ψηφοφόρος να πουλήσει την ψήφο του, ή να γίνει ο ίδιος θύμα εξαναγκασμού για να ψηφίσει με συγκεκριμένο τρόπο. Έτσι ο Benaloh και ο Tuinstra [7] έδωσαν το πρώτο πρωτόκολλο ηλεκτρονικής ψηφοφορίας που ήταν “Receipt free”. Ακολούθησαν και άλλες προτάσεις που είχαν την ιδιότητα του “ Receipt free”, όπως του Tatsuaki Okamoto[10], των Byoungcheon Lee και Kwangjo Kim [11], καθως και των Emmanouil Magkos, Mike Burmester, και Vassilios Chrissikopoulos[12]. Ένα μειονέκτημα τέτοιων πρωτοκόλλων ήταν το γεγονός ότι έκαναν μη πρακτικές υποθέσεις, όπως η υπόθεση ύπαρξης καναλιών επικοινωνίας στα οποία ο επιτιθέμενος δεν έχει καθόλου πρόσβαση.

Σαν προέκταση της ιδιότητας receipt freeness, παρουσιάζεται από τους Juels, Catalano και Jakobsson, η ιδιότητα coercion resistance. Στην εργασία[23] μπορεί ο αναγνώστης να εντοπίσει ένα σαφή διαχωρισμό των ιδιοτήτων receipt freeness και coercion resistance .Εργασία με στόχο την επίλυση του προβλήματος εξαναγκασμού στις εκλογές έγινε και από τους Kutylowski και Zagorski[13] . Στο [25] ο Ralf Kusters και Tomasz Truderung δίνουν ένα αυστηρό ορισμό του coercion resistance, παρουσιάζοντας τις αδυναμίες κάποιων συστημάτων που έχουν προταθεί προς επίλυση του προβλήματος εξαναγκασμού. Πιο πρόσφατα, το 2013 και 2014, προτείνονται δύο συστήματα [21][22] τα οποία κτίζουν πάνω στο Civitas, με σκοπό την βελτίωση του και την επίλυση του προβλήματος εξαναγκασμού .

2.3 Παραδείγματα χρήσης διαδυκτιακών εκλογικών συστημάτων

Η ψηφοφορία μέσω διαδικτύου εφαρμόζεται στην Εσθονία [5] [6], ως ένας εναλλακτικός τρόπος ψηφοφορίας, με ένα σημαντικό ποσοστό των ψηφοφόρων της να την προτιμά.



Σχήμα 2.1 πηγή : eGovernance Academy ,σύνδεσμος: http://www.ega.ee/node/835

Όπως φαίνεται στην πιο πάνω παράσταση, σε κάθε νέα εκλογική αναμέτρηση από το 2005 που ξεκίνησε η εφαρμογή του συστήματος, ο αριθμός των ψηφοφόρων που προτιμούν την ηλεκτρονική ψηφοφορία αυξάνεται σημαντικά. Το σύστημα που χρησιμοποιείται στην Εσθονία είναι προσβάσιμο μέσω του συνδέσμου: https://www.valimised.ee/eng/ ενώ στον σύνδεσμο: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/, μπορούν να βρεθούν περισσότερα στατιστικά στοιχεία σχετικά με τις διαδικτυακές εκλογές στην Εσθονία.

Για τους σκοπούς της ηλεκτρονικής ψηφοφορίας το 2002 , το Κοινοβούλιο της Εσθονίας επέβαλε την αντικατάσταση των ταυτοτήτων με ηλεκτρονικές ταυτότητες, μέσω της οποίας μπορούσε να γίνει η ψηφοφορία. Για να μπορεί κάποιος να ψηφίσει μέσω διαδικτύου πρέπει :

1. Να έχει σύνδεση στο διαδίκτυο
2. Να χρησιμοποιεί ένα από τα 3 λειτουργικά συστήματα, Windows, MacOS ή Linux
3. Να έχει την ηλεκτρονική τους ταυτότητα και τον κωδικό PIN
4. Να έχει ένα ηλεκτρονικό υπολογιστή που να έχει είτε το ειδικό λογισμικό , είτε ένα smart card reader.

Αν ένας ψηφοφόρος αποφασίσει να ψηφίσει με χαρτί σε κανονική κάλπη, μπορεί αλλά θα ακυρωθεί οποιαδήποτε ψήφος καταχωρήθηκε μέσω του διαδικτύου, έστω και αν γίνει σε μεταγενέστερο στάδιο. Σε περίπτωση που ο χρήστης ψηφίζει μόνο διαδικτυακά και ψηφίσει πάνω από μια φορά, μετρά πάντα η τελευταία.

Ένα ακόμη παράδειγμα διαδικτυακής ψηφοφορίας είναι το σύστημα Helios, το οποίο δίνει την δυνατότητα σε οποιαδήποτε επιθυμεί να επαληθεύσει την εγκυρότητα των αποτελεσμάτων. Το σύστημα είναι προσβάσιμο μέσω του συνδέσμου https://vote.heliosvoting.org/. Το σύστημα σύμφωνα με τους σχεδιαστές του απέχει πολύ από το να μπορεί να χρησιμοποιηθεί σε εθνικές εκλογές. Μπορεί να χρησιμοποιηθεί σε εκλογικές διαδικασίες όπου δεν υπάρχουν απαιτήσεις για άμυνα έναντι του εξαναγκασμού. Το σύστημα επιλέγει να δώσει στους χρήστες την δυνατότητα να επαληθεύσουν τα αποτελέσματα, θυσιάζοντας την ιδιότητα της αντίστασης στον εξαναγκασμό. Στον σύνδεσμο https://acm2014.heliosvoting.org/ μπορεί κάποιος να δει ότι το Helios όντως χρησιμοποιείται από οργανισμούς για εκλογικές διαδικασίες. Ένα σύστημα με το ΖΕΥΣ βασισμένο στο Helios αναπτύσσεται από την ελληνική κυβέρνηση και είναι προσβάσιμο μέσω του συνδέσμου: https://zeus.minedu.gov.gr

Κεφάλαιο 3

Κρυπτογραφία

Σε αυτή την ενότητα παρουσιάζονται θέματα κρυπτογραφίας τα οποία χρησιμοποιούνται από το συστήμα Civitas το οποίο θα εξεταστεί στην συνέχεια.

3.1 Σύστημα κρυπτογράφησης ElGamal

Το συγκεκριμένο σύστημα προτάθηκε από τον Taher ElGamal ως μια επέκταση του πρωτοκόλλου Diffie–Hellman key exchange από τους Whitified Diffie και Martin Hellman. Έτσι προτού παρουσιαστεί το σύστημα κρυπτογραφίας ElGamal θα παρουσιαστεί το πρωτόκολλο ανταλλαγής κλειδιού από τους Whitified Diffie και Martin Hellman, ενώ θα παρουσιαστούν και κάποιες μαθηματικές έννοιες, χρήσιμες για την κατανόηση των πρωτοκόλλων που παρουσιάζονται.

3.1.1 Θεωρεία αριθμών

Σε αυτή την υπο-ενότητα στόχος είναι να παρουσιαστούν κάποιες μαθηματικές έννοιες, χρήσιμες για την κατανόηση συστημάτων κρυπτογράφησης δημοσίου κλειδιού. Θα αναφερθούν όσα χρειάζονται για να γίνει κατανοητό το σύστημα κρυπτογράφησης ElGamal.

Σημειογραφία:

N -> Θετικός ακέραιος

p -> πρώτος αριθμός

Z_N = { 0,1,2,..., N-1}.

Σε αυτό το σύνολο ορίζουμε τις πράξεις πρόσθεσης και πολλαπλασιασμό (ορίζουμε δηλαδή

δακτύλιο) πάντα κάνοντας τις με mod N ,ώστε το αποτέλεσα να βρίσκεται επίσης στο σύνολο Z_N .

Για παράδειγμα, αν N=12 τότε :

9+8 στο Z_N = (9+8) mod N = 5 στο Z_N

5*7 στο Z_N = (5*7) mod N = 11 στο Z_N

5-7 στο Z_N = (5-7) mod N = 2 στο Z_N

Μέγιστος κοινός διαιρέτης

gcd (x,y) : Μέγιστος κοινός διαιρέτης των x,y.

Για κάθε x,y υπάρχουν ακέραιοι a,b τέτοιοι ώστε gcd (x,y) = a*x+b*y.

Οι αριθμοί a,b μπορούν να βρεθούν με την χρήση του επεκταμένου Ευκλείδειου αλγόριθμου.

Αν gcd (x,y)=1 τότε οι αριθμοί x,y λέγοντα σχετικά πρώτοι

Αντίστροφοι αριθμοί στο Z_N

Ο αντίστροφος ενός αριθμού x (όπου x ανήκει στο Z_N) είναι ένας αριθμός y(όπου y ανήκει στο Z_N) έτσι ώστε x*y=1 στο Z_N .

Όμως δεν έχει κάθε στοιχείο του συνόλου Z_N αντίστροφο.

Λήμμα : Για κάθε στοιχείο x του συνόλου Z_N ισχύει ότι έχει αντίστροφο αν και μόνο αν gcd (x,N)=1 , δηλαδή είναι σχετικά πρώτος με το πλήθος του συνόλου αυτού.

Επιπλέον ορίζουμε το σύνολο Z_N* ως το σύνολο που περιέχει τα στοιχεία του συνόλου Z_N. τα οποία έχουν αντίστροφο. Συγκεκριμένα :

$Z_N^* = \{x \in Z_N \mid gcd(x,N) = 1\}$

Θεώρημα του Φερμά (1640)

Έστω p πρώτος αριθμός.

Για κάθε στοιχείο $x \in (Z_p^*)$ ισχύει ότι $x^{p-1}=1$ στο Z_p

Επιπλέον ο Euler μας πληροφορεί πως το σύνολο (Z_p^*) είναι κυκλική ομάδα (cyclic group) ,δηλαδή υπάρχει μέλος g , του συνόλου αυτού, το οποίο μπορεί να παράξει όλα τα μέλη του συνόλου . Το μέλος αυτό ονομάζεται γεννήτορας. Συγκεκριμένα:

(Z_p^*) οριζεται κυκλική ομάδα, δηλαδή $\exists\, g \in (Z_p^*)$ τέτοιο ώστε

$\{g0, g1, g2, g3, \ldots, gp-2\} = (Z_p^*)$

Το σύνολο που παράγεται από το γεννήτορα g συμβολίζεται με <g>, και λέμε ότι το order του

γεννήτορα $g \in (Z_p^*)$ ισούται με το πλήθος του συνόλου <g> που παράγει , δηλαδή:
$ord_p(g) = |\langle g \rangle|$, όπου $g \in (Z_p^*)$.

Από τον Joseph-Louis Lagrange πληροφορούμαστε πως
$\forall g \in (Z_p)^*$:$ord_p(g)$ διαιρεί τον αριθμό p-1.

3.1.2 Ανταλλαγή κλειδιού Diffie–Hellman

Έστω η Alice και ο Bob , δύο άτομα που πρώτη φορά γνωρίζονται και θέλουν να ανταλλάξουν μεταξύ τους κρυπτογραφημένες πληροφορίες. Για να το κάνουν αυτό θα πρέπει να υπάρχει ένα κλειδί το οποίο θα τους επιτρέπει να κρυπτογραφούν τις συγκεκριμένες πληροφορίες. Αφού όμως πρώτη φορά γνωρίζονται, τέτοιο κλειδί δεν υπάρχει και θα πρέπει να δημιουργήσουν νέο.
Το πρωτόκολλο Diffie-Hellman είναι σε θέση να δώσει λύση στο πρόβλημα αυτό. Στόχος του είναι ο υπολογισμός του κλειδιού από οποιονδήποτε άλλον εκτός από την Alice και τον Bob να γίνεται σε χρόνο εκθετικό, και άρα μη πρακτικό.

Το πρωτόκολλο έχει ως εξής:
1.Καθορισμός μιας πεπερασμένης κυκλικής ομάδας G ($G=(Z_p^*)$) πλήθους n.
2. Επιλογή αριθμού **g** ,γεννήτορα της προαναφερθήσας κυκλικής ομάδας.
3. Η Alice επιλέγει αριθμό **α** από το σύνολο {x| x>=1 και x<=n}.
4. Ο Bob επιλέγει αριθμό **β** από το σύνολο {x| x>=1 και x<=n}.
5. Η Alice υπολογίζει ($A=g^a \mod p$), και το στέλνει στον Bob.
6. Ο Bob υπολογίζει ($B=g^b \mod p$), και το στέλνει στην Alice.
7. Η Alice λαμβάνει το B, και υπολογίζει $K_{\alpha\beta}=B^a \mod p=g^{ab} \mod p$.
8. Ο Bob λαμβάνει το A, και υπολογίζει $K_{\alpha\beta}=A^b \mod p=g^{ab} \mod p$.
Αποτέλεσμα της πιο πάνω διαδικασίας είναι ο Bob και η Alice να καταλήγουν σε ακριβώς το ίδιο κλειδί. Κάποιος που παρακολουθεί το κανάλι επικοινωνίας μεταξύ των δύο αυτών ατόμων , μπορεί να παρατηρήσει και να γνωρίζει τα ακόλουθα:
$p, g, g^a \mod p, g^b \mod p$

Η αποτελεσματικότητα του συγκεκριμένου πρωτοκόλλου βασίζεται στο γεγονός ότι παρόλο που γνωρίζει τις πιο πάνω τιμές, χρειάζεται εκθετικό χρόνο για να υπολογίσει ο ίδιος το κλειδί $K_{\alpha\beta}$,αφού χρειάζεται να εξάγει το **a** από το **$g^a \mod p$**,και το **b** από το **$g^b \mod p$**.

3.1.3 Ανταλλαγή κλειδιού ElGamal

Το συγκεκριμένο πρωτόκολλο ανταλλαγής κλειδιού στηρίζεται στο πρωτόκολλο Diffie–Hellman .

1.Καθορισμός μιας πεπερασμένης κυκλικής ομάδας G ($G=(Z_p^*)$) πλήθους n.

2. Επιλογή αριθμού g ,γεννήτορα της προαναφερθήσας κυκλικής ομάδας.

3. Η Alice κατασκευάζει το δημόσιο κλειδί της ως εξης:
επιλέγει αριθμό a από το σύνολο {x| x>=1 και x<=n}.
υπολογίζει ($A=g^a \mod p$) και θέτει το A ως δημόσιο κλειδί.

4. Ο Bob κατασκευάζει το δημόσιο κλειδί της ως εξης:
επιλέγει αριθμό b από το σύνολο {x| x>=1 και x<=n}.
υπολογίζει ($B= g^a \mod p$) και θέτει το B ως δημόσιο κλειδί.

5. Όταν ο Bob θέλει να επικοινωνήσει με την Alice , παίρνει το δημόσιο της κλειδί A, και υπολογίζει $K_{\alpha\beta}=A^b \mod p=g^{ab} \mod p$. Ακολούθως στέλνει στην Alice το εξής:
[B,E(m,$K_{\alpha\beta}$). Δηλαδή κρυπτογραφεί το μήνυμα m , με το κλειδί $K_{\alpha\beta}$, και το στέλνει μαζί με το δικό του δημόσιο κλειδί B. Η Alice για να αποκρυπτογραφήσει το μήνυμα, πρέπει να υπολογίσει το κλειδί $K_{\alpha\beta}$ ως εξης: $K_{\alpha\beta}=B^a$. Έχοντας το κλειδί, αποκρυπτογραφεί και διαβάζει το μήνυμα.

6. Όταν η Alice θέλει να επικοινωνήσει με τον Bob κάνει την αντίστοιχη εργασία με αυτή που έκανε ο Bob.

Στο πιο πάνω πρωτόκολλο, τα ιδιωτικά και δημόσια κλειδιά έχουν ως εξής:

	Alice	Bob
Ιδιωτικό	a	b
Δημόσιο	g^a	g^b

Η αποτελεσματικότητα έγκειται στο γεγονός ότι οποιοσδήποτε καταγράφει την επικοινωνία στο κανάλι μεταξύ του Bob και της Alice, είναι αδύνατον (από άποψη χρόνου) για αυτόν να καταφέρει να υπολογίσει τα ιδιωτικά κλειδιά a και b, γνωρίζοντας τα g^a και g^b .

3.2 Πρωτόκολλα μηδενικής γνώσης

Η σκοπός των πρωτοκόλλων μηδενικής γνώσης [14] [15] [16] είναι σχετικά απλός:

Ο Bob αποδεικνύει στην Alice ότι γνωρίζει ένα μυστικό χωρίς να αποκαλύπτει κάποια πληροφορία σχετικά με το μυστικό. Η Alice θα θέσει μια σειρά δοκιμασιών στον Bob, και αν ο Bob της περάσει με επιτυχία, η Alice μπορεί να υπόθεσει πως ο Bob όντως γνωρίζει το μυστικό. Ο λόγος που η Alice υποθέτει και δεν είναι βέβαιη, είναι πως ο Bob ενδέχεται να απάντησε τυχαία σωστά σε όλες τις δοκιμασίες της Alice. Η πιθανότητα να συμβεί κάτι τέτοιο μειώνεται, όσο αυξάνεται ο αριθμός και η δυσκολία των δοκιμασιών που θέτει η Alice.

Η απαιτήσεις ενός συστήματος ψηφοφορίας, το οποίο είναι σχεδιασμένο με τρόπο ώστε να επιτρέπει σε όποιονδίποτε να ελέγξει την ορθότητα των αποτελέσματων, οδηγούν στην υιοθέτηση μη διαδραστικών αποδείξεων μηδενικής γνώσης. Πρώτα όμως ας καθορίσουμε τι εννοούμε λέγοντας διαδραστικές αποδείξεις μηδενικής γνώσης.

Από το [16] πληροφορούμαστε ότι οι διαδραστικές αποδείξεις μηδενικής γνώσης, βασίζονται σε τυχαιοποιημένο πρωτόκολλο πολλών γύρων , το οποίο εκτελείται από δύο μέρη, αυτόν που θέλει να απόδειξη ότι κατέχει ένα μυστικό (prover) και αυτόν που προσπαθεί να επαληθεύσει τον ισχυρισμό του πρώτου (verifier). Το πρωτόκολλο πρέπει να είναι τέτοιο ώστε:

α) Να επιτρέπει στον ισχυριζόμενο να αποδείξει την γνώση του μυστικού . (Ιδιότητα **completeness**)
β) Καμία τακτική του ισχυριζόμενου να μην είναι ικανή να ξεγελάσει τον επαληθευτή. (Ιδιότητα **soundness**).

Αφού λοιπόν σε ένα διαδραστικό πρωτόκολλο παίρνουν μέρος δύο μέρη, τότε για την ορθότητα των αποτελεσμάτων της ψηφοφορίας μπορεί κάθε φορά να πεισθεί ένας επαληθευτής σε κάθε εκτέλεση του πρωτοκόλλου, ότι όντως τα αποτελέσματα είναι ορθά. Αφού όμως τα συστήματα ψηφοφοριών απαιτούν την ιδιότητα “publicly verifiable”, δεν είναι βολική η υιοθέτηση ενός διαδραστικού πρωτοκόλλου αποδείξεων μηδενικής γνώσης.

Η λύση στο πρόβλημα έρχεται μέσα από την χρήση μη-διαδραστικών αποδείξεων μηδενικής γνώσης, όπως τις πρότειναν ο Fiat και Shamir [17] . Η κεντρική ιδέα πίσω από τις μη διαδραστικές αποδείξεις μηδενικής γνώσης, και που τις κάνει ιδανικές για την υλοποίηση της ιδιότητας “publicly

verifiable”, είναι πως πλέον δεν υπάρχουν 2 μέρη στο πρωτόκολλο, παρά μόνο ο επαληθευτής, που προσπαθεί να επαληθεύσει την ορθότητα της απόδειξης που τοποθετήθηκε μαζί με τα αποτελέσματα των εκλογών.

3.3 Διαμοιρασμός μυστικού μηνύματος

Όπως θα αναλυθεί σε μεταγενέστερη ενότητα , σε συστήματα ψηφοφορίας , υπάρχει η ανάγκη διαμοιρασμού κάποιου μυστικού, κατά την διάρκεια της εγγραφής του χρήστη πριν την εκλογική αναμέτρηση. Το μυστικό αυτό είναι το ιδιωτικό κλειδί που χρησιμοποιεί ο ψηφοφόρος κατά την διάρκεια της ψηφοφορίας. Σε αυτή την υπο-ενότητα θα παρουσιαστεί εν συντομία η μέθοδος που προτάθηκε από τον Adi Shamir το 1979 [18] και κάνει εφικτό τον διαμοιρασμό μυστικού.

Το πρόβλημα μπορεί να παρουσιαστεί μέσω παραδείγματος ως εξής :

“Έντεκα επιστήμονες δουλεύουν σε ένα μυστικό project. Θέλουν να κλειδώσουν τα αρχεία τους σε ένα δωμάτιο , με τρόπο τέτοιο που η καμπίνα να μπορεί να ανοίξει μόνο στην παρουσία 6 ή περισσοτέρων επιστημόνων. Ποιος είναι ο μικρότερος αριθμός κλειδαριών που χρειάζονται; Ποιος είναι ο μικρότερος αριθμός κλειδιών που πρέπει να κουβαλά κάθε ένας από τους επιστήμονες;” [19]

Δεδομένου ενός ζεύγους (k,n), στόχος είναι να σπάσουμε το μυστικό D σε n κομμάτια , έτσι ώστε:

1. Αν κάποιος γνωρίζει k ή περισσότερα κομμάτια του μυστικού D , να μπορεί εύκολα να υπολογίσει ολόκληρο το μυστικό και
2. Αν κάποιος γνωρίζει λιγότερα από k κομμάτια του μυστικού D , να μην είναι σε θέση να υπολογίσει το μυστικό.

Κατά την φάση της εγγραφής, και παραγωγής του ιδιωτικού κλειδιού του ψηφοφόρου, ισχύει ότι k=n. Το κλειδί σπάζει σε n κομμάτια (ένα από κάθε υπεύθυνο εγγραφής), και για να είναι σε θέση κάποιος να γνωρίζει το κλειδί χωρίς να το μάθει από τον ίδιο τον χρήστη, πρέπει να έχει και τα n κομμάτια. Αυτός είναι ο λόγος που στο JCJ/Civitas υπάρχει η απαίτηση, ότι ανάμεσα στους υπεύθυνους εγγραφής χρειάζεται τουλάχιστο ένας να είναι έμπιστος, έτσι ώστε να μην μπορούν να συγκεντρωθούν και τα n κομμάτια και άρα να αποκαλυφθεί το ιδιωτικό κλειδί του χρήστη.
Η διαδικασία στηρίζεται στην παρεμβολή πολυωνύμων :

n+1 σημεία του επιπέδου (x_i,y_i), για κάθε i που ανήκει στο σύνολο {x|x>=0 ^x<=n}.
Υπάρχει μοναδικό πολυώνυμο p(x) βαθμού το πολύ n, τέτοιο ώστε:
$p(x_i)= y_i$, για κάθε i που ανήκει στο σύνολο {x|x>=0 ^x<=n}.

Έτσι για να χωρίσουμε το μυστικό σε n κομμάτια, επιλέγεται ένα πολυώνυμο p k-1 βαθμού, στο οποίο ισχύει a0=S, όπου S το μυστικό.

p(x)=a0+a1*x+a2*x2 + … ak-1*x(k-1)

Ακολούθως υπολογίζουμε:
S1=p(1), S2=p(2) … Si=p(i) … Sn=p(n) .

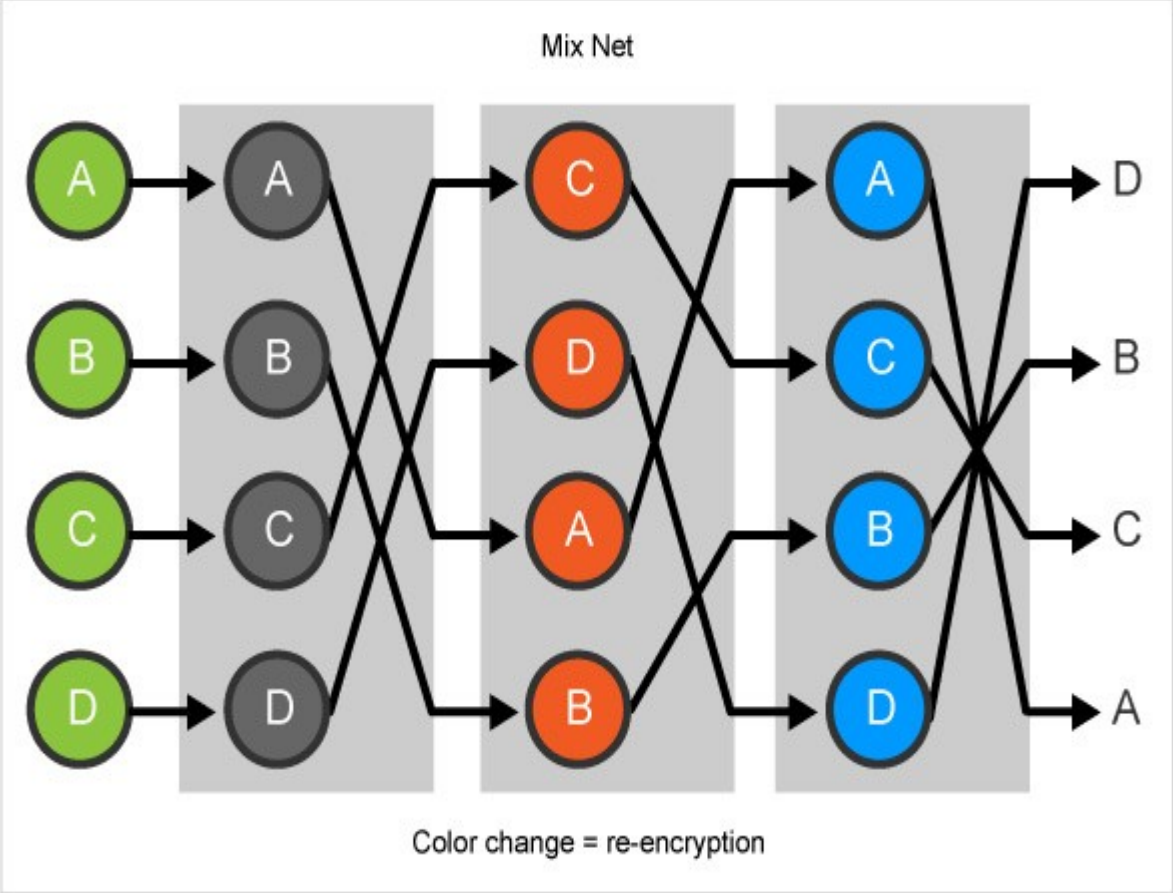
3.4 Δίκτυα μίξης (mixnets)

Τα δίκτυα μίξης παρουσιάστηκαν πρώτη φορά από τον David Chaum το 1981[20]
Τα δίκτυα μίξης , είναι χρήσιμα αφού συντελούν στην δημιουργεία ανώνυμων καναλιών , που χρειάζονται σε συστήματα εκλογών μέσω διαδυκτίου. Στόχος είναι τα μηνύματα που εξάγονται από ένα δίκτυο μίξης , να μην μπορούν να αντιστοιχηστούν στα μηνύματα που εισήχθηκαν σε αυτό. Αν δεν υπήρχαν τα δίκτυα μίξης, κάποιος που παρακολουθεί το κανάλι επικοινωνίας μεταξύ του ψηφοφόρου και του εξυπηρετητή στο σύστημα , δεν θα μπορούσε μεν να δει τι ψήφισε ο χρήστης, θα μπορεί να ξέρει όμως ότι ψήφισε. Άρα τίθεται σαν στόχος να χρησιμοποιηθούν τα mixnets με τρόπο τέτοιο που να είναι αδύνατον σε όποιον παρακολουθεί ένα κανάλι επικοινωνίας , να αντιληφθεί την πηγή και τον προορισμό ενός μηνύματος. Αν κάποιος παρακολουθεί τον υπολογιστή της Alice και βλέπει ένα μήνυμα να εξέρχεται από αυτόν προς το διαδίκτυο, δεν θα πρέπει να είναι σε θέση να γνωρίζει ότι το μήνυμα κατευθύνεται προς τον εξυπηρετητή των εκλογών, και εάν παρακολουθεί το δίκτυο στο οποίο βρίσκεται ο εξυπηρετητής , δεν θα πρέπει να είναι σε θέση να αντιληφθεί από που προέρχεται κάθε ψήφος.

Κάθε εξυπηρετητής δικτύου μίξης, λαμβάνει ένα σύνολο μηνυμάτων τα οποία επανα-κρυπτογραφεί , και πραγματοποιεί τυχαία αναμετάθεση μεταξύ των μηνυμάτων , με στόχο τα μηνύματα εξόδου να μην μπορούν να αντιστοιχησθούν σωστά με τα μηνύματα εισόδου.

Επιπλέον οπως θα παρουσιαστεί αργότερα ,τα δίκτυα μίξης χρησιμοποιούνται ως τεχνική

απόδειξης μηδενικής γνώσης με την οποία όποισδίποτε θα μπορεί να επαληθεύσει τα αποτελέσματα των εκλογών



Σχήμα 3.1 πηγή: http://www.wombat-voting.com/how-to-vote/verifiability

Κεφάλαιο 4

Πρόβλημα εξαναγκασμού στις εκλογικές αναμετρήσεις.

Ένα από τα προβλήματα που πρέπει να αντιμετωπιστούν , ώστε να γίνουν πραγματικότητα οι εκλογικές αναμετρήσεις μέσω διαδικτυακών συστημάτων, είναι αυτό του εξαναγκασμού . Αφού δίνεται η δυνατότητα, ο κάθε ψηφοφόρος να ψηφίζει από όποιο μέρος επιθυμεί , προκύπτει το πρόβλημα πως, σε εκείνο το μέρος δεν θα είναι απαραίτητα μόνος του. Επίσης, την ώρα που ψηφίζει, μπορεί κάποιος να βρίσκεται μαζί του και να τον παρακολουθεί να ψηφίζει.

Η πρώτη αναφορά στο πρόβλημα αυτό γίνεται από τους,Benaloh και ο Tuinstra [7] ,οι οποίοι παρατήρησαν πως η ένδειξη που δινόταν στον ψηφοφόρο και στο οποίο αναγραφόταν το τι ψήφισε, μπορούσε να χρησιμοποιηθεί ώστε ο ψηφοφόρος να αποδείξει ότι ψήφισε με συγκεκριμένο τρόπο. Κάτι τέτοιο οδηγούσε σε πωλήσεις ψήφων ή και σε εξαναγκασμό των ψηφοφόρων να ψηφίσουν με συγκεκριμένο τρόπο. Έτσι ο Benaloh και ο Tuinstra [7] έδωσαν το πρώτο πρωτόκολλο ηλεκτρονικής ψηφοφορίας που ήταν “Receipt free”. Αργότερα εισάγεται ένας πιο αυστηρός ορισμός της συγκεκριμένης απειλής, από τους Juels, Catalano and Jakobsson, δίνοντας την ιδιότητα του coercion resistance. Λίγα χρόνια αργότερα, παρουσιάζεται το σύστημα Civitas , που στηρίζετα στη λύση που έδωσαν οι Juels, Catalano και Jakobsson, και το οποίο εξασφαλίζει πως ο επιτιθέμενος δεν θα έχει καμία ένδειξη για το αν ο ψηφοφόρος όντως ακολούθησε τις οδηγίες του, έστω και αν τον είδε να ψηφίζει. Το συγκεκριμένο σύστημα όμως φαίνεται να είναι μη πρακτικό , εξαιτίας των μη ρεαλιστικών υποθέσεων που κάνει. Γιαυτό τον λόγο, προτάθηκαν αρκετές βελτιώσεις στο συγκεκριμένο σύστημα. Αν ο αναγνώστης θέλει να εξετάσει τον πηγαίο κώδικα του συστήματος, μπορεί να το πράξει μέσω του συνδέσμου: http://www.cs.cornell.edu/projects/civitas/

4.1 Civitas

Κεντρικοί στόχοι του συστήματος Civitas , είναι να ικανοποιεί τις εξής απαιτήσεις :

α) Η ψηφοφορία να γίνεται μέσω διαδικτύου .
β) Να υπάρχει άμυνα έναντι επιθέσεων εξαναγκασμού
γ) Το τελικό αποτέλεσμα πρέπει να μπορεί να επαληθευτεί από οποιονδήποτε, και επιπλέον κάθε ψηφοφόρος να μπορεί να επαληθεύσει ότι όντως , η δική του ψήφος μετρήθηκε σωστά.

Προτού σχεδιαστεί το σύστημα που θα πληρεί τις πιο πάνω απαιτήσεις, χρειάζεται να καθοριστούν οι δυνατότητες του επιτιθέμενου, ώστε να γίνουν πιο ευδιάκριτοι οι μηχανισμοί άμυνας που πρέπει να ενσωματωθούν . Οι δυνατότητες του επιτιθέμενου έχουν ως εξής:

- Μπορεί να επηρεάσει και να κατευθύνει ένα συγκεκριμένο αριθμό συστατικών του συστήματος, προς τον δικό του σκοπό. Τα συστατικά αυτά μπορεί να είναι είτε άνθρωποι, είτε προγράμματα.
- Μπορεί να αναγκάσει τους ψηφοφόρους να ψηφίσουν με ένα συγκεκριμένο τρόπο , ή να παραδώσουν τα συνθηματικά τους, ή να μην ψηφίσουν καθόλου. Υπάρχει όμως η απαίτηση ότι ο επιτιθέμενος δεν θα μπορεί να είναι καθόλη την διάρκεια των εκλογών μαζί με τον ψηφοφόρο, αφού ο ψηφοφόρος δεν θα μπορεί να εγγραφή ή και να ψηφίσει.
- Ο επιτιθέμενος μπορεί να ελέγχει όλα τα δημόσια κανάλια. Υπάρχουν όμως κανάλια στα οποία ο επιτιθέμενος δεν έχει καθόλου πρόσβαση.
- Ο επιτιθέμενος είναι σε θέση να κάνει υπολογισμούς πολυωνυμικού χρόνου.

Οι κατηγορίες ατόμων που αποτελούν μέρος του συστήματος είναι οι εξής:

- Επόπτης εκλογών: Είναι υπεύθυνος για την έναρξη και λήξη των εκλογών, και την συνολική λειτουργία του συστήματος
- Γραμματέα:εγκρίνει τους ψηφοφόρους
- Υπεύθυνοι εγγραφών: αλληλεπιδρούν με τους ψηφοφόρους με σκοπό την παραγωγή δημοσίου και ιδιωτικού κλειδιού. Η χρήση των κλειδιών θα εξηγηθεί στην συνέχεια.
- Καταμετρητές ψήφων: Αθροίζουν τους ψήφους

Το Civitas χωρίζει την διαδικασία σε τρις φάσεις:

- Φάση προετοιμασίας και ρύθμισης
- Φάση ψηφοφορίας
- Φάση καταμέτρησης ψήφων

Επιπλέον για την σωστή λειτουργία του συστήματος, γίνονται οι εξής υποθέσεις:

1. Ο εχθρός δεν μπορεί να προσποιηθεί τον ψηφοφόρο κατά την διάρκεια της εγγραφής.
2. Κάθε ψηφοφόρος εμπιστεύεται τουλάχιστον ένα υπεύθυνο εγγραφής, και το κανάλι από τον ψηφοφόρο στον έμπιστο υπεύθυνο εγγραφής, είναι ασφαλές.
3. Οι ψηφοφόροι εμπιστεύονται τις μηχανές στις οποίες ψηφίζουν.
4. Τα κανάλια που χρησιμοποιούνται για την αποστολή των ψήφων στο σύστημα, διατηρούν τον ψηφοφόρο ανώνυμο.
5. Τουλάχιστον μια κάλπη στην οποία τοποθετούνται ψήφοι , λειτουργεί σωστα.
6. Υπάρχει τουλάχιστον ένας έντιμος καταμετρητής ψήφων.
7. Το SHA-256, το Decision Diffie-Hellman και RSA χρησιμοποιούν τυχαιότητα για παραγωγεί τον κλειδιών.

4.2 Κεντρική ιδέα για την αντιμετώπιση του εξαναγκασμού

Κατά την διάρκεια εγγραφής ενός πολίτη ως ψηφοφόρου, για να μπορεί να ψηφίσει στις εκλογές, παράγονται δύο συνθηματικά, το ένα δημόσιο και το άλλο ιδιωτικό. Το δημόσιο συνθηματικό τοποθετείται στο “bulletin board”, δηλαδή σε πίνακα , στον οποίο τοποθετούνται όσα δεδομένα χρειάζονται ώστε να είναι δυνατή η επαλήθευση των αποτελεσμάτων . Το ιδιωτικό συνθηματικό αποτελείται από n κομμάτια. Κάθε κομμάτι εξασφαλίζεται από έναν υπεύθυνο εγγραφής. Έχοντας ένα κομμάτι από κάθε υπεύθυνο εγγραφής, εκτελεί ένα αλγόριθμο ο οποίος παράγει το ιδιωτικό συνθηματικό. Η μυστικότητα του συνθηματικού, βασίζεται στην μέθοδο διαμοιρασμού μυστικού που περιγράφηκε στην υπο-ενότητα 3.3 . Έτσι μόνο εάν συναινέσουν όλοι οι υπεύθυνοι εγγραφής, μπορεί το συνθηματικό να διαρρεύσει. Γιαυτό τον λόγο γίνεται η υπόθεση ότι υπάρχει τουλάχιστο ένας έμπιστος/έντιμος υπεύθυνος εγγραφών , που δεν θα συναινέσει να δώσει το δικό του μερίδιο από το τελικό συνθηματικό.

Κατά την διάρκεια της ψηφοφορίας, όταν ο ψηφοφόρος επιθυμεί να ψηφίσει, πρέπει να καταχωρήσει μαζί με την ψήφο του και το πιο πάνω ιδιωτικό συνθηματικό. Η αποτελεσματικότητα

λοιπόν της μεθόδου, έγκειται στο γεγονός ότι όταν βρίσκεται υπό την πίεση να ψηφίσει με συγκεκριμένο τρόπο, το πράττει με ψεύτικο συνθηματικό. Το ψεύτικο συνθηματικό πρέπει να είναι τέτοιο που ο επιτιθέμενος να μην είναι σε θέση να το διακρίνει από ένα πραγματικό . Έτσι όταν ο ψηφοφόρος βρίσκεται υπό πίεση πράττει ως εξής :

Ο επιτιθέμενος αναγκάζει τον ψηφοφόρο να:	**Ο ψηφοφόρος :**
Ψηφίσει με συγκεκριμένο τρόπο	Παράγει ψεύτικο ιδιωτικό συνθηματικό και ψηφίζει όπως επιθυμεί ο επιτιθέμενος
Να πωλήσει , ή να παραδώσει το ιδιωτικό συνθηματικό του	Παράγει ψεύτικο ιδιωτικό συνθηματικό και το παραδίδει στον επιτιθέμενο.
Να απέχει από τις εκλογές	Παράγει ψεύτικο ιδιωτικό συνθηματικό και το παραδίδει στον επιτιθέμενο.

Πίνακας 3.1.1

Ως αποτέλεσμα , ο επιτιθέμενος μη γνωρίζοντας αν το συνθηματικό που έλαβε από τον ψηφοφόρο, ή το συνθηματικό που είδε τον ψηφοφόρο να καταχωρεί, είναι αληθινό ή ψεύτικο, δεν έχει κανένα λόγο να πιστέψει πως ο ψηφοφόρος ακολούθησε πιστά τις οδηγίες του.

4.3 Ανάλυση φάσεων του συστήματος

1. Φάση προετοιμασίας και ρύθμισης

Η συγκεκριμένη φάση είναι κρίσιμη για την αποτελεσματικότητα του συστήματος , αφού σε αυτή θα παραχθούν τα ιδιωτικά συνθηματικά των χρηστών .

Ο επόπτης , δημιουργεί νέα εκλογική διαδικασία, αναρτώντας τον σχεδιασμό του ψηφοδελτίου στην ιστοσελίδα. Επιπλέον καθορίζει τους ψηφολέκτες, αναρτώντας τα δημόσια κλειδιά τους. Η γραμματέας αναρτά των εκλογικό κατάλογο, που περιέχει τους νόμιμους ψηφοφόρους , μαζί με τα δημόσια κλειδιά τους. Παράλληλα οι καταμετρητές των ψήφων δημιουργούν από κοινού ένα δημόσιο κλειδί. Το δημόσιο κλειδί πρέπει να είναι τέτοιο που οτιδήποτε κρυπτογραφήθηκε με αυτό, να χρειάζεται την συναίνεση όλων των καταμετρητών για να αποκρυπτογραφηθεί . Τέλος, το σημείο κλειδί για την αντιμετώπιση του εξαναγκασμού, η παραγωγή των συνθηματικών κάθε ψηφοφόρου. Παράγεται ένα δημόσιο και ένα ιδιωτικό συνθηματικό. Το δημόσιο συνθηματικό

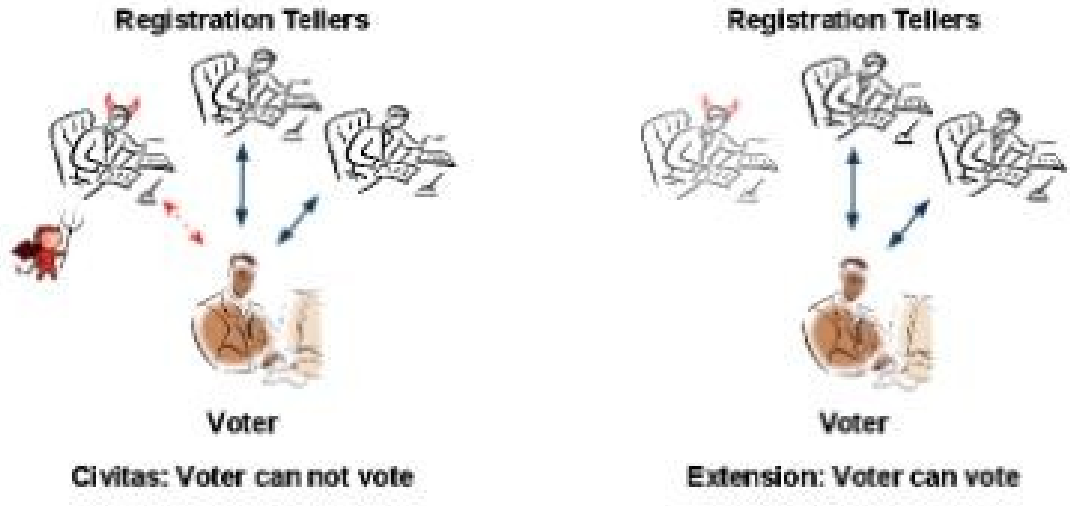
αναρτάται στο bulettin board, ώστε κάθε ψηφοφόρος να είναι σε θέση να ελέγξει ότι η ψήφος που μετρήθηκε για τον ίδιο όντως αντιστοιχεί σε αυτό που ο ίδιος ψήφισε. Για την κατασκευή των ιδιωτικών κλειδιών, κάθε υπεύθυνος εγγραφής, παρέχει το δικό του κομμάτι στον ψηφοφόρο. Ο ψηφοφόρος τρέχει αλγόριθμο ο οποίος συνδυάζει τα συνθηματικά , και παράγει το τελικό συνθηματικό, που θα χρησιμοποιήσει την ώρα που ψηφίζει.

Για αυτή την φάση γίνονται κάποιες υποθέσεις που καθιστούν το Civitas μη πρακτικό στον πραγματικό κόσμο. Η επίλυση των συγκεκριμένων υποθέσεων θα φέρουν το Civitas ένα βήμα πιο κοντά στην αξιοποίηση του από τον πραγματικό κόσμο. Οι πρώτες δύο υποθέσεις είναι :

Υπόθεσεις εμπιστοσύνης 1,2:

1. Ο εχθρός δεν μπορεί να προσποιηθεί τον ψηφοφόρο κατά την διάρκεια της εγγραφής.

2. Κάθε ψηφοφόρος εμπιστεύεται τουλάχιστον ένα υπεύθυνο εγγραφής , και το κανάλι από τον ψηφοφόρο στον έμπιστο υπεύθυνο εγγραφής, είναι ασφαλές.



Σχήμα 4.1 πηγή: [26]

Στο [25] (ενότητα 5.2) , οι Ralf Kusters και Tomasz Truderung , εντοπίζουν πως υπό τις συνθήκες που περιγράφηκε η συγκεκριμένη φάση όταν προτάθηκε για πρώτη φορά το Civitas, δεν αντιμετώπιζε πλήρως το πρόβλημα του εξαναγκασμού .

Σε περίπτωση που ένας χρήστης έχει σκοπό να ψηφίσει ένα συγκεκριμένο υποψήφιο, μπορεί να μην

τα καταφέρει, αφού υπάρχει το σενάριο πως δεν θα καταφέρει καν να εγγραφεί και να εξασφαλίσει από κάθε υπεύθυνο εγγραφής κομμάτι από το ιδιωτικό συνθηματικό. Αυτό θα γίνει αν ο επιτιθέμενος επικοινωνεί με κάποιο υπεύθυνο εγγραφής, ο οποίος θα τον ενημερώσει για το αν ο ψηφοφόρος έχει πάρει από αυτόν το κομμάτι του ιδιωτικού κλειδιού ή όχι. Ο επιτιθέμενος αναγκάζει τον ψηφοφόρο να μην πάρει το συγκεκριμένο κομμάτι ιδιωτικού κλειδιού, γιατί σε αντίθεση περίπτωση θα ενημερωθεί από τον υπεύθυνο εγγραφής και θα υπάρχουν συνέπειες. Ως αποτέλεσμα ο ψηφοφόρος δεν μπορεί να εγγραφεί και άρα δεν μπορεί να ψηφίσει.

Επιπλέον , υπάρχει το ενδεχόμενο , ένας μη έμπιστος υπεύθυνος εγγραφής, να δώσει λάθος κομμάτι συνθηματικού στον ψηφοφόρο (σκόπιμα), το οποίο όμως να συσχετίζεται σωστά με το δημόσιο συνθηματικό . Σε τέτοια περίπτωση ο ψηφοφόρος είναι με την εντύπωση ότι κατέχει σωστό ιδιωτικό συνθηματικό ενώ στην πραγματικότητα χρησιμοποιεί ένα λανθασμένο.

Εξαιτίας αυτών των αδυναμιών που εντοπίστηκαν στην αρχική έκδοση του Civitas, στο [26] , προτείνεται αλλαγή στην διαδικασία παραγωγής των ιδιωτικών συνθηματικών . Η αλλαγή βασίζεται στο ότι ο ψηφοφόρος αλληλεπιδρά μόνο με υπεύθυνους εγγραφής τους οποίους εμπιστεύεται και εξασφαλίζει μόνο από αυτούς κομμάτια του ιδιωτικού συνθηματικού . Ο χρήστης πρέπει να αποφασίσει από πριν ποιους εμπιστεύεται ώστε να κάνει αίτημα για συνθηματικό μόνο σε αυτούς. Το τελικό συνθηματικό θα παράγεται από τα κομμάτια που θα παρθούν από τους έμπιστους υπεύθυνους εγγραφής. Με αυτή την ιδέα, στο [26] , προτείνουν την αντικατάσταση της δεύτερης υπόθεσης με την ακόλουθη:

Νέα υπόθεση εμπιστοσύνης 2:
Ο ψηφοφόρος εμπιστεύεται ένα σύνολο υπευθύνων εγγραφής , του οποίου το πλήθος είναι μεγαλύτερο των μισών υπευθύνων εγγραφής . Επιπρόσθετα , το κανάλι από τον ψηφοφόρο σε τουλάχιστο ένα έμπιστο υπεύθυνο εγγραφής είναι ασφαλές.

Κατά τη άποψη του γράφοντος, η προτεινόμενη λύση στο [26] , δεν εγγυάται την επίλυση του προβλήματος για τους εξής λόγους:

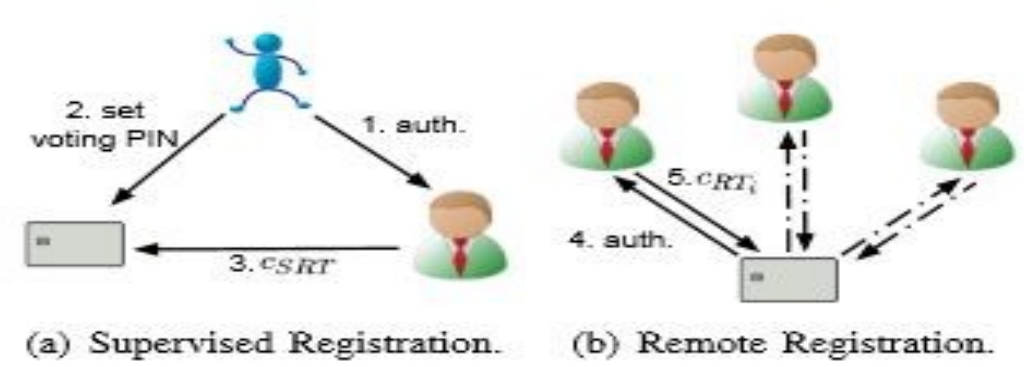
α) Ένας ψηφοφόρος ενδέχεται να μην έχει τόσα άτομα που να εμπιστεύεται στο σύνολο των υπευθύνων εγγραφής. Για να ψηφίσει θα αναγκαστεί να προσθέσει άτομα που δεν εμπιστεύεται ώστε να εξασφαλίσει κομμάτι συνθηματικού από περισσότερους των μισών υπευθύνων εγγραφής.

Ένα άτομο από αυτά που πρόσθεσε για να μπορέσει να ψηφίσει ενδέχεται συνεργάζεται με τον επιτιθέμενο.

β) Όπως γίνονταν και στην αρχική έκδοση του Civitas, η όλη λύση εξαρτάται από την εντιμότητα των ανθρώπων που τέθηκαν σαν υπεύθυνοι εγγραφής. Στις πιο πάνω επιθέσεις που αναφέρθηκαν , χρειάζεται μόνο ένα άτομο μη έμπιστο , από το σύνολο των “έμπιστων” , για να καταστρέψει την λύση.

Οι Stephan Neumann και Melanie Volkamer, στην εργασία τους [24] , αναλύουν τις 2 πρώτες υποθέσεις . Παρόλο που η ύπαρξη ενός ασφαλούς καναλιού επικοινωνίας είναι μείζονος σημασίας στην λύση που δίνεται από το Civitas, στην πραγματικότητα είναι δύσκολο να υπάρξει ένα τόσο ασφαλές κανάλι επικοινωνίας . Επιπλέον στην πρώτη υπόθεση αν ένας ψηφοφόρος θέλει να πωλήσει την ψήφο του, και εφόσον η εγγραφή γίνεται εξ αποστάσεως, μπορεί μαζί του , κατά την διάρκεια της εγγραφής να είναι ο επιτιθέμενος . Ή αν ο επιτιθέμενος θέλει να μάθει το ιδιωτικό κλειδί και να είναι σίγουρος για αυτό, μπορεί να αναγκάσει τον ψηφοφόρο να πραγματοποιήσει την εγγραφή μπροστά του. Σε κάθε περίπτωση , ο επιτιθέμενος μπορεί να είναι μαζί με το θύμα μόνο κατά την διάρκεια της εγγραφής, και να μάθει αμέσως το πραγματικό ιδιωτικό κλειδί. Άρα προκύπτει πως η πρώτη υπόθεση δεν είναι καθόλου ρεαλιστική, αφού αν ο επιτιθέμενος θέλει όντως να αναγκάσει τον ψηφοφόρο να ακολουθήσει τις οδηγίες του, θα φροντίσει να είναι μαζί του κατά την διάρκεια της εγγραφής. Η απάντηση στο πρόβλημα αυτό σύμφωνα με το [24] , είναι η εγγραφή να γίνεται μερικώς εξ αποστάσεως και μερικώς προσωπικά.

Για να εγγραφεί ένας χρήστης, πρέπει να συναντηθεί με έναν επικεφαλή υπεύθυνο εγγραφών. Ο επικεφαλής αυτός θα βεβαιωθεί ότι ο ψηφοφόρος δεν ελέγχεται εκείνη την στιγμή από κάποιον επιτιθέμενο. Η ταυτότητα του ψηφοφόρου πιστοποιείται χρησιμοποιώντας την προσωπική του έξυπνη κάρτα , eID. Ακολούθως καταχωρεί στην κάρτα το PIN του , ώστε ο επικεφαλής να είναι σε θέση να καταχωρήσει το συνθηματικό του ψηφοφόρου σε αυτήν. Ακολούθως ο χρήστης , εξ αποστάσεως χρησιμοποιεί την κάρτα για να εξασφαλίσει τα υπόλοιπα κομμάτια του ιδιωτικού συνθηματικού, εξ αποστάσεως .



Σχήμα 4.2 πηγή : [24] – Figure 2 Voter-Process

Ως αποτέλεσμα της πιο πάνω προσέγγισης της διαδικασίας εγγραφής , η πρώτη υπόθεση, καθώς και το δεύτερο μέρος της δεύτερης υπόθεσης (που αφορά το ασφαλές κανάλι), μετατρέπετε στην εξής:

Νέα υπόθεση εμπιστοσύνης 1:
Κάθε χρήστης εμπιστεύεται τον επικεφαλή των υπευθύνων εγγραφής, και τουλάχιστο τους μισούς υπευθύνους εγγραφής.

2. Φάση ψηφοφορίας

Στην αρχική έκδοση του Civitas, ο ψηφοφόρος συνδυάζει τα ιδιωτικά συνθηματικά που εξασφάλισε από κάθε ένα από τους υπεύθυνους εγγραφών, και τρέχοντας συγκεκριμένο αλγόριθμο , κατασκευάζει το ιδιωτικό συνθηματικό. Πλέων με το συνθηματικό έτοιμο είναι σε θέση να ψηφίσει, όποτε επιθυμεί, πριν την λήξη των εκλογών. Σε περίπτωση που αναγκαστεί ή δωροδοκηθεί να πράξει με συγκεκριμένο τρόπο, ο ψηφοφόρος μπορεί να δράσει όπως περιγράφεται στον πίνακα 3.1.1 .

Για να ψηφίσει ο χρήστης , καταχωρεί το ιδιωτικό συνθηματικό που κατασκεύασε μαζί με την ψήφο του. Επιπλέον καταχωρεί απόδειξη πως η ψήφος είναι σωστά καταχωρημένη . Τα τρία αυτά συστατικά της καταχώρησης, τοποθετούνται σε πολλές ηλεκτρονικές κάλπες ώστε να εξασφαλίζεται διαθεσιμότητα .

Οι χρήστες ενδέχεται να θέλουν να ψηφίσουν ξανά . Ο υπεύθυνος εκλογών έχει την ευχέρεια να αποφασίσει με πια πολιτική θα χειριστεί τέτοιες περιπτώσεις. Αν η επανα-κατάθεση ψήφου δεν επιτρέπετε τότε , ακυρώνονται όλες οι ψήφοι και μετρά μόνο η πρώτη.

Το Civitas , είναι συμβατό με κάθε ψηφοδέλτιο σχεδιασμένο με τρόπο που μπορεί να αποδειχθεί η καταλληλότητα του. Αν το ψηφοδέλτιο είναι τέτοιο ώστε να μπορούν να αριθμηθούν οι υποψήφιοι κατά σειράν προτίμησης τότε, μπορεί να φέρει αδυναμία στο σύστημα , και επιθέσεις εξαναγκασμού . Αυτή η απειλή μπορεί να περιοριστεί .Επιπλέον μπορούσε να υπάρχει η επιλογή, οι χρήστες να γράφουν το όνομα του/των επιλογών , αλλά κάτι τέτοιο έχει εμφανέστατα προβλήματα εξαναγκασμού , και δεν υπάρχει μέχρις στιγμής κάποιος γνωστός τρόπος που να κάνει τέτοιου είδους ψηφοδέλτια κατάλληλα για διαδικτυακές ψηφοφορίες .Μια υπόθεση που γίνεται σχετικά με την φάση της ψηφοφορίας είναι :

Υπόθεση εμπιστοσύνης 3:
Οι ψηφοφόροι εμπιστεύονται πλήρως τους υπολογιστές στους οποίους ψηφίζουν.

Πρόκειται φυσικά για μη ρεαλιστική υπόθεση αφού :

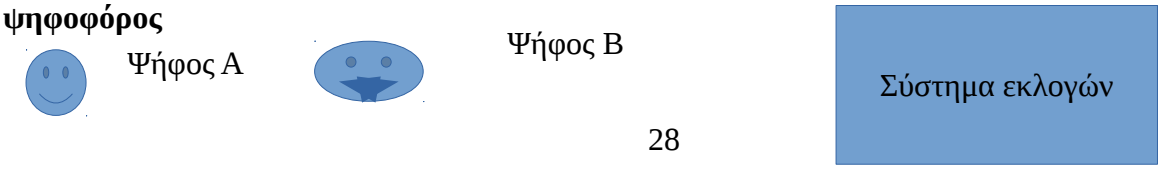
Μπορεί ο επιτιθέμενος να έχει εντοπίσει ευπάθεια σε οποιοδήποτε λογισμικό τρέχει στον υπολογιστή του ψηφοφόρου, και εκμεταλλευόμενος αυτή να την παραβίασε και να απέκτησε πρόσβαση στο σύστημα. Μπορεί κάποιος “έμπιστος” που έχει πρόσβαση στον υπολογιστή, να τοποθέτησε σκόπιμα κακόβουλο λογισμικό

Το υλικό του υπολογιστή ή το τοπικό δίκτυο ενδέχεται να ελέγχονται από τον επιτηθέμενο.
Αυτό μπορεί να έχει ως αποτέλεσμα να διαρρεύσει ο τρόπος με τον οποίο ψήφισε ο χρήστης, ή/και να ψηφίσει στην θέση του χρήστη . Όλα αυτά φυσικά , εν αγνοία του χρήστη. Επομένως γίνεται σαφές ότι ένα σύστημα που υποθέτει ότι ο ψηφοφόρος έχει απόλυτη εμπιστοσύνη στον υπολογιστή του, δεν μπορεί να θεωρηθεί ασφαλές.

Εάν ο χρήστης δεν θέλει να διαρρεύσει ο τρόπος με τον οποίο ήθελε να ψηφίσει, τότε μπορεί να ψηφίσει πάνω από μια φορές, ώστε αν κάποιος όντως παρακολουθεί την δραστηριότητα του, να μην μπορεί να ξέρει ποια από τις ψήφους ήταν αυτή με το σωστό συνθηματικό . Αντιθέτως αν ψηφίσει μόνο μια φορά θα μπορεί ο επιτιθέμενος - κατάσκοπος να είναι σχεδόν βέβαιος ότι η συγκεκριμένη ψήφος είναι έγκυρη. Αναφέρω “σχεδόν βέβαιος” και όχι βέβαιος, αφού αν κάποιος ψηφίσει μόνο μια φορά, και είναι με την εντύπωση πως δεν απειλείται / παρακολουθείται, τότε πιθανότατα (και όχι σίγουρα) θα ψηφίσει σωστά.

Η δοκιμή Benaloh μπορεί να χρησιμοποιηθεί για να βεβαιώσει τους χρήστες ότι η ψήφος που τελικά καταχωρήθηκε αντιστοιχεί στην ψήφο που οι ίδιοι καταχώρησαν. Με βάση την δοκιμή Benaloh, η διαδικασία της ψηφοφορίας, χωρίζεται σε δυο επιμέρους φάσεις. Στην πρώτη, ο ψηφοφόρος καταχωρεί την επιλογή του και παίρνει σαν απάντηση την κρυπτογραφημένη ψήφο. Όμως η ψήφος δεν αποθηκεύεται στο σύστημα ως επιλογή του χρήστη. Το σύστημα αμέσως μετά την καταχώρηση του χρήστη (δεύτερη φάση), δίνει στον χρήστη την επιλογή να αποθηκεύσει την ψήφο του , ή να “δοκιμάσει” το σύστημα. Αν ο χρήστης επιλέξει να “δοκιμάσει” το σύστημα, τότε το σύστημα θα πρέπει να εξάγει απόδειξη για το ότι όντως το σύνολο χαρακτήρων που εξήγαγε ως κρυπτογραφημένη ψήφο, αντιστοιχεί στην ψήφο του χρήστη. Με αυτή την απόδειξη ο χρήστης μπορεί να ελέγξει ότι η ψήφος του και η κρυπτογραφημένη ψήφος που πήρε από το σύστημα συμφωνούν. Αυτό γίνεται στα πλαίσια της προσπάθειας για να επιτευχθεί επαλήθευση του συστήματος. Έστω ότι σε μια εκλογική αναμέτρηση , οι υποψήφιοι είναι ο Α, ο Β, και ο Γ. Ο χρήστης καταχωρεί Α, αλλά το σύστημα επιστρέφει Ε(Β), δηλαδή την κρυπτογράφηση της ψήφου Β. Φυσικά ο χρήστης αν δεν γνωρίζει πως έγινε η κρυπτογράφηση δεν θα μπορεί να ξέρει ότι το σύνολο χαρακτήρων που πήρε σαν απάντηση δεν αντιστοιχεί στην δική του κρυπτογραφημένη επιλογή αλλά στην επιλογή Β. Έτσι για τον συγκεκριμένο χρήστη θα καταχωρηθεί Β και όχι Α, και ο ίδιος βλέποντας στον πίνακα ανακοινώσεων την τιμή Ε(Β) , δίπλα από τον αριθμό ταυτότητας του, θα συμφωνήσει ότι όντως αυτή ήταν η τιμή που καταχώρησε στο σύστημα , αλλά δεν θα γνωρίζει ότι αυτή η τιμή δεν ήταν η επιλογή του. Σαφώς ένα τέτοιο σύστημα δεν πληρεί την απαίτηση της ακεραιότητας. Με την ιδιότητα της επαληθευσημότητας όμως παρέχεται η δυνατότητα στον χρήστη να βεβαιωθεί ο ίδιος ότι η επιλογή του καταχωρείται ορθά στο σύστημα, και να διαπιστώσει ο ίδιος αν είναι ή όχι το σύστημα “ακέραιο”. Ο χρήστης μπορεί να “δοκιμάσει” όσες φορές θέλει το σύστημα, μέχρι να πειστεί ότι το σύστημα χειρίζεται σωστά την ψήφο του. Όμως όταν ο χρήστης πείθετε ότι το σύστημα είναι ακέραιο και θέλει να αποθηκεύσει την ψήφο του (δεύτερη φάση), το σύστημα δεν θα του επιστρέψει απόδειξη για το ότι η κρυπτογραφημενη ψήφος αντιστοιχεί στην επιλογή του επειδή αυτή μπορεί να χρησιμοποιηθεί για να αποδείξει ο ψηφοφόρος σε κάποιον άλλο για το πως ψήφισε.

Στην πιο πάνω υπόθεση όμως αναφέρεται ότι ο ψηφοφόρος εμπιστεύεται πλήρως την μηχανή στην οποία ψηφίζει. Αν όμως ο υπολογιστής είναι μολυσμένος, ή υπό τον έλεγχο ενός επιτιθέμενου, μπορεί να συμβεί το εξής :



Ο νόμιμος ψηφοφόρος ψηφίζει αλλά η ψήφος του δεν καταλήγει ποτέ στο σύστημα, εξαιτίας του κακόβουλου λογισμικού/επιτηθέμενου, που φροντίζει να ψηφίσει εκ μέρους του, ή να μην καταχωρηθεί καθόλου ψήφος. Έτσι για αυτό τον λόγο, και επειδή το κακόβουλο λογισμικό μπορεί να επιρεάσει και την φάση της “δοκιμής” του συστήματος όπως αναφέρθηκε πιο πάνω (δοκιμή Benaloh/ Benaloh challenge) ,προτύνεται στο [24] η δοκιμή να γίνεται από διαφορετικό υπολογιστή, με την ελπίδα ότι ο δεύτερος δεν θα είναι μολυσμένος με κακόβουλο λογισμικό. Φυσικά αυτό δεν λύνει το πρόβλημα της ύπαρξης κακόβουλων λογισμικών, αλλά θα βοηθήσει στην “χαλάρωση” της πιό πάνω υπόθεσης, η οποία μετατρέπεται στην εξής :

Νέα υπόθεση εμπιστοσύνης 3

Ο επιτιθέμενος δεν μπορεί να ελέγχει ταυτόχρονα τον υπολογιστή στον οποίο ψηφίζει ο χρήστης και τον υπολογιστή/κινητό μέσω του οποίου ελέγχεται το αν καταχωρήθηκε η σωστή ψήφος.

Στο [24], κωδικοποιώντας την ψήφο με τυχαιότητα σε ένα Qr-code μπορεί να μειώσει την εξάρτηση από την εμπιστοσύνη του χρήστη στον υπολογιστή του. Κατασκευάζοντας το προαναφερθέν Qr-code, ο χρήστης μπορεί να το σαρώσει με το κινητό του και να διαπιστώσει την ορθότητα της ψήφους που καταχωρήθηκε. Με αυτό το τρόπο απαιτείται να είναι είτε ο υπολογιστής χωρίς κακόβουλο λογισμικό, ή το κινητό (ώστε μέσω αυτού να μπορεί να εντοπιστεί πιθανή ασυμφωνία μεταξύ της ψήφου που καταχώρησε ο χρήστης και της ψήφου που καταχωρήθηκε στο σύστημα) . Δεν είναι απαραίτητη η χρήση Qr-code και κινητού όπως αναφέρεται στο [24], φτάνει η δοκιμή να γίνεται από διαφορετικό μηχάνημα από αυτό της επιλογής ψήφου. Αν ο χρήστης πράξει με αυτό το τρόπο και όντως ο επιτιθέμενος/κακόβουλο λογισμικό δεν μπορεί να ελέγχει και τις δύο μηχανές, θα εντοπιστεί ασυμφωνία κατά την φάση της δοκιμής Benaloh. Η χρήση μιας συσκευής που να μην μπορεί να επιρεαστεί από κακόβουλο λογισμικό θα ηταν ιδανική για χρήση κατά την φάση της “δοκιμής” του συστήματος.

Επιπλέον σε αυτή την φάση γίνεται η εξής υπόθεση:

Υπόθεση εμπιστοσύνης 4:

Τα κανάλια επικοινωνίας μέσω των οποίων οι ψηφοφόροι καταχωρούν την ψήφο τους , φροντίζουν να διατηρούν την πηγή της ψήφου (διεύθηνση IP του ψηφοφόρου) μυστική.

Σε αντίθετη περίπτωση μπορεί κάποιος να μάθει ποιοί ψήφισαν (όχι όμως τι ψήφισαν αφού η ψήφος είναι κρυπτογραφημένη). Επειδή τέτοια ανώνυμα κανάλια δεν έχουν ακόμα υλοποιηθεί, οι σχεδιαστές του Civitas [27] προτύνουν την χρήση του δικτύου Tor.

3. Φάση καταμέτρησης:

1. Κάθε υπεύθυνος υπολογισμού, παίρνει τις ψήφους από τις ηλεκτρονικές κάλπες και τα δημόσια συνθηματικά από το bulettin board.

2. Ελέγχονται οι αποδείξεις για να πιστοποιηθεί η καταλληλότητα της ψήφου και του ψηφοφόρου. Κάθε ψήφος με λάθος απόδειξη δεν μετριέται.

3. Μόνο μια ψήφος για κάθε ψηφοφόρο λαμβάνεται υπόψιν, με βάση την πολιτική που ακολουθείται για την διαχείριση πολλών ψήφων από ένα ψηφοφόρο ,και φυσικά με βάση το αληθινό ιδιωτικό συνθηματικό που καταχώρησε ο χρήστης. Όμως επειδή το ιδιωτικό συνθηματικό δεν επιτρέπεται να διαρρεύσει, γίνεται χρήση του πρωτοκόλλου PET (plaintext equivalence test), για σύγκρηση των κρυπτογραφημένων ψήφων. Το πρωτόκολλο PET ελέγχει αν για δύο κρυπτογραφημένα κείμενα c και c' , ισχύει Dec(c)=Dec(c') , δηλαδή αν αποκρυπτογραφούνται στο ίδιο κείμενο (ψήφο για την συγκεκριμένη περίπτωση).

4. Γίνεται χρήση δικτύων μίξης, με σκοπό να διασφαλιστεί η ανωνυμία στο σύνολο των έγκυρων συνθηματικών και των καταχωρημένων ψήφων. Κάθε υπεύθυνος υπολογισμού κάνει την δική του αναμετάθεση στα στοιχεία του προαναφερθέν σύνολου.

6. Οι εναπομείναντες επιλογές αλλά όχι τα συνθηματικά αποκρυπτογραφούνται, και το τελικό αποτέλεσμα μπορεί να υπολογιστεί /επαληθευτεί από όποιον το επιθυμεί μέσω του bulettin board.
Κάθε υπεύθυνος καταμέτρησης είναι αναγκασμένος να αναρτήσει αποδείξεις για το γεγονός ότι ακολούθησε πλήρως του πρωτόκολλο, και κάθε ένας μπορεί να ελέγξει αυτές τις αποδείξεις κατά την διάρκεια της καταμέτρησης, ή μετά από αυτήν. Ο κάθε ψηφοφόρος μπορεί επίσης να ελέγξει ότι η δική του ψήφος είναι ορθή και μέρος του αποτελέσματος

4.4 Επαληθευσιμότητα αποτελεσμάτων

Σε ένα σύστημα ψηφοφορίας υπάρχει η απαίτηση όπως τα τελικά αποτελέσματα που εξάγει το σύστημα είναι επαληθεύσιμα. Με αυτό εννοείται το εξής:

- Κάθε χρήστης είναι σε θέση να επαληθεύσει ότι η ψήφος του καταχωρήθηκε στο σύστημα όπως αυτός ήθελε.

- Κάθε χρήστης είναι σε θέση να επαληθεύσει ότι στο τελικό αποτέλεσμα λαμβάνεται η ψήφος του με τον τρόπο που ο ίδιος την καταχώρησε στο σύστημα.

- Κάθε χρήστης είναι σε θέση να επαληθεύσει ότι το τελικό αποτέλεσμα είναι όντως σωστό, δηλαδή ότι όλες οι ψήφοι μετρήθηκαν όπως ακριβως καταχωρήθηκαν.

- Κάθε χρήστης είναι σε θέση να επαληθεύσει ότι όσοι ψήφισαν, όντως δικαιούνταν να ψηφίσουν

Ένα τέτοιο σύστημα χαρακτηρίζεται ως “End to End Verifiable Voting System”.
Στις πλείστες εκλογικές διαδικασίες , από την στιγμή τοποθέτησης της ψήφου και μετά, ο ψηφοφόρος δεν έχει αντίληψη για το τι γίνεται με εκείνη την ψήφο. Εμπιστεύεται την σωστή διαχείριση της ψήφου, σε άτομα τα οποία δεν γνωρίζει, και δεν ξέρει καν αν η ψήφος του μετρήθηκε σωστά ή όχι.

Σαφώς ένας τρόπος να γίνει αυτό, είναι αμέσως μετά τις εκλογές να εκτυπωθούν σε εφημερίδες όλες οι ταυτότητες των ψηφοφόρων και δίπλα τι ακριβώς ψήφισαν , ώστε ο κάθε ένας να είναι σε θέση να ελέγξει τόσο την δική του ψήφο, όσο και το τελικό αποτέλεσμα, και χωρίς μάλιστα να χρειάζεται να εμπιστευτεί τον οποιοδήποτε.

Αριθμός ταυτότητας	**Ψήφισε**
993165	Ναι
994065	Όχι
99350435	Όχι
99312355	Όχι

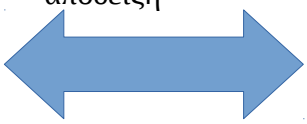
Πινακας 4.1

Κάτι τέτοιο όμως παραβιάζει την μυστικότητα ψήφου, και μπορεί να οδηγήσει σε αγοραπωλησίες ψήφων, αφού ο ψηφοφόρος έχει εύκολο τρόπο να αποδείξει τι ακριβώς ψήφισε . Αρα η ερώτηση που προκύπτει είναι η εξής:

Μπορούμε να παρέχουμε σε ένα ψηφοφόρο την δυνατότητα να επαληθεύσει τα αποτελέσματα , κρατώντας την ψήφο μυστική;

Η απάντηση είναι θετική, και εδώ μπαίνει η χρησιμότητα της κρυπτογραφίας και συγκεκριμένα των αποδείξεων μηδενικής γνώσης. Όταν ένας χρήστης ψηφίσει, πέρνει την ψήφο του κρυπτογραφημένη (σε αυτό το σημείο ο αναγνώστης καλείται να θυμηθεί την έννοια του Receipt freenes που αναφέρθηκε σε προηγούμενη υποενότητα). Έτσι αφού η ψήφος είναι κρυπτογραφημένη, θα μπορεί να ελέγξει στο τέλος των εκλογών και αφού αναρτηθούν οι ψήφοι στο bulletin board, αν η κρυπτογραφημένη ψήφος που βλέπει στον πίνακα με τα αποτελέσματα αντιστοιχεί στην κρυπτογραφημένη ψήφο που έλαβε από το σύστημα.

Αριθμός ταυτότητας	**Ψήφισε**
993165	odlspf
994065	djafhn
99350435	wrerdf
99312355	vbx



Αποτέλεσμα:

Όχι: 3
Ναι: 1

Σχήμα 4.3 Κρυπτογραφημένες ψήφοι για να διατηρείται η μυστικότητα ψήφου

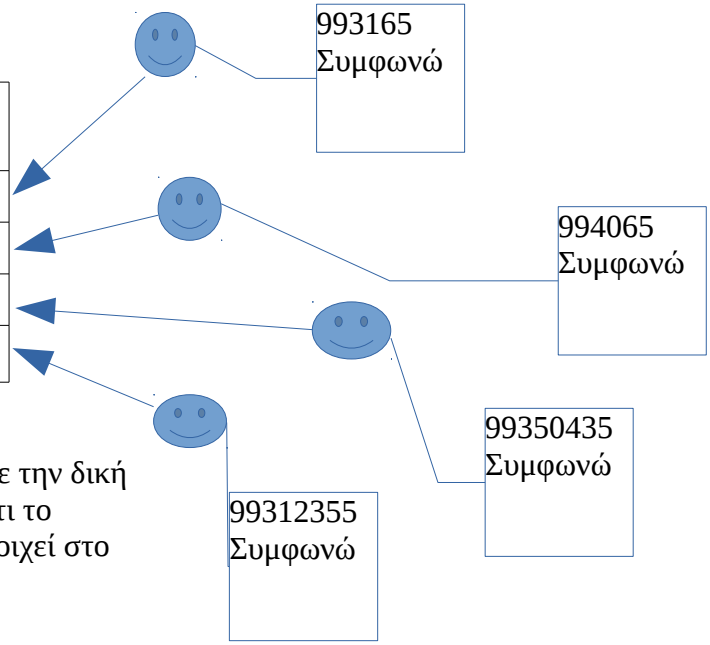
Αφού κάθε ψηφοφόρος μπορεί να πιστοποιήσει πως η ψήφος που βλέπει είναι όντως αυτή που

καταχώρησε, πρέπει να πιστοποιηθεί ότι όντως αυτή η ψήφος μετρήθηκε από το σύστημα. Για να γίνει αυτό πρέπει να εφαρμόσει μαθηματική απόδειξη πάνω στο σύνολο των ψήφων για να αποδείξει ότι όντως με βάση τις ψήφους που είναι δημοσιευμένες , αθροίζονται σωστά τα αποτελέσματα. Αν γίνει αυτό τότε γίνεται το εξής:

Οι ψηφοφόροι συμφωνούν με τα δημοσιευμένα αποτελέσματα της δικής τους ψήφου.
Τα δημοσιευμένα αποτελέσματα στο σύνολο τους, αποδεδειγμένα συμφωνούν με τα τελικά αποτελέσματα της καταμέτρησης.
Άρα οι ψηφοφόροι πείθονται ότι η δική τους σωστή ψήφος μέτρησε στο τελικό αποτέλεσμα.
Άρα το σύστημα είναι επαληθεύσιμο .

Βήμα 1:

Αριθμός ταυτότητας	**Ψήφισε**
993165	odlspf
994065	djafhn
99350435	wrerdf
99312355	vbx



Βήμα 2: Αφού όλοι συμφωνούν με την δική τους ψήφο, μένει να αποδειχθεί ότι το σύνολο αυτών των ψήφων αντιστοιχεί στο τελικό αποτέλεσμα

Σχήμα 4.4

Η απόδειξη που εφαρμόζεται στο σύνολο των ψήφων είναι μη διαδραστική απόδειξη μηδενικής γνώσης με την χρήση δικτύων μήξης ή μπορεί να γίνεται χρήση ομομορφικής κρυπτογράφισης. Στην ομομορφική κρυπτογράφηση, υπάρχει η πράξη της πρόσθεσης (modulo ένα μεγάλο αριθμό) και η πράξη του πολλαπλασιασμού (modulo ένα μεγάλο αριθμό), τέτοιες ώστε το «γινόμενο» των κρυπτογραφήσεων οποιωνδήποτε δύο ψήφων, να ισούται με την κρυπτογράφηση του «αθροίσματος» των ψήφων:
E(v1)*E(v2) mod P = E(v1+v2) mod P

Παρόλο όμως που μπορεί επιτευχθεί επαλήθευση των αποτελεσμάτων προκύπτουν τα εξής προβλήματα:

α) Κάποιος βλέποντας τις δημοσιευμένες ψήφους μπορεί να ξέρει ποιοι ψηφίσαν
β) Οποιοσδήποτε μπορεί να δει την κρυπτογραφημένη ψήφο οποιουδήποτε ψηφοφόρου.

Γιατί τα πιο πάνω σημεία δημιουργούν πρόβλημα:

α) Έστω ότι ο Μποπ απειλεί την Αλίκη να **μην** ψηφίσει. Η Αλίκη όμως ψηφίζει. Ο Μποπ μπορεί να το μάθει στο τέλος των εκλογών με την δημοσίευση των κρυπτογραφημένων ψήφων. Δεν θα μάθει πως ψήφισε αλλά θα ξέρει ότι ψήφισε, κάτι που μπορεί να οδηγήσει σε φαινόμενα εξαναγκασμού.

β) Έστω ότι η Αλίκη ψηφίζει μόνη της αυτό που πραγματικά θέλει να ψηφίσει. Το σύστημα της επιστρέφει την κρυπτογραφημένη ψήφο, ώστε να μπορεί αργότερα να γίνει επαλήθευση των αποτελεσμάτων. Η Αλίκη έχει αριθμό ταυτότητας 993165 (από το Σχήμα 4.2 πιο πάνω) , και η κρυπτογράφηση της ψήφου της είναι : “odlspf“ (από το Σχήμα 4.2 πιο πάνω) . Αργότερα ο Μποπ αναγκάζει την Αλίκη να ψηφίσει μπροστά του με συγκεκριμένο τρόπο. Η Αλίκη ξεγελά τον Μποπ αλλά το σύστημα, για σκοπούς επαλήθευσης αποτελεσμάτων , επιστρέφει την κρυπτογραφημένη ψήφο του Μποπ που είναι : “poropspe”. Για σκοπούς επαλήθευσης των αποτελεσμάτων δημοσιεύονται οι κρυπτογραφημένες ψήφοι. Η Αλίκη βλέπει ότι αυτό που της επέστρεψε το σύστημα όντως αντιστοιχεί στην ψήφο που είναι δημοσιευμένη δίπλα από την ταυτότητα της , δηλαδή “odlspf“ , και είναι ευχαριστημένη. Ο Μποπ όμως μπορεί να δει και ο ίδιος ότι η κρυπτογραφημένη ψήφος της Αλίκης έχει τιμή “odlspf“ και όχι “poropspe” , άρα αντιλαμβάνεται ότι η Αλίκη τον ξεγέλασε.

Μέσα από τα πιο πάνω παραδείγματα μπορεί να γίνει πιο εύκολα κατανοητή η σύγκρουση που υπάρχει ανάμεσα στην επαλήθευση των αποτελεσμάτων και στην μυστικότητα ψήφου:

Πως θα δώσουμε την ευκαιρία στην Αλίκη να βεβαιωθεί ότι η ψήφος της μετρήθηκε σωστά, ενώ ταυτόχρονα διατηρούμε τον Μποπ πεπεισμένο ότι η Αλίκη ακολούθησε τις δικές του οδηγίες πιστά;

Στο Civitas οι καταμετρητές ψήφων είναι αναγκασμένοι να καταθέτουν αποδήξεις ότι ακολούθούν την πιο πάνω διαδικασία καταμέτρησης σωστά. Αρκεί να υπάρχει ένας έντιμος καταμετρητής ψήφων ο οποίος θα αρνηθεί να συνεχίσει αν εντοπίσει λάθος απόδειξη αναρτημένη από άλλον καταμετρητή , ώστε η φάση καταμέτρησης να είναι σωστή. Όποιοσδίποτε μπορεί να ελέγχει τις αποδείξης κατά την διάρκεια της καταμέτρησης ή και μετά από αυτήν. Επίσης κάθε ψηφοφόρος μπορεί να βεβαιοθεί ότι η ψήφος του είναι στο σύνολο καταμέτρησης. Το σύστημα έτσι προσφέρει την δυνατότητα σε όποιον το επιθυμεί να επαληθεύσει την ορθότητα των αποτελεσμάτων.

4.5 Συμπέρασμα

Όπως προαναφέρθηκε, όταν προτάθηκε για πρώτη φορά το Civitas απαιτούνταν να ισχύει ότι ο επιτιθέμενος δεν μπορεί να προσποιηθεί τον ψηφοφόρο, και υπάρχει κάποια χρονική περίοδος κατά την οποία ο ψηφοφόρος απαιτείται να είναι μόνος του, ώστε σε αυτό το κομμάτι να εκτελέσει μέρος της εγγραφής. Επιπλέον στην δεύτερη υπόθεση διευκρίνιζε πως πρέπει να υπάρχει ασφαλές κανάλι μεταξύ του ψηφοφόρου και ενός υπευθύνου εγγραφών κατά την διάρκεια της ψηφοφορίας.

Εξηγήθηκε επίσης ο λόγος για τον οποίο οι συγκεκριμένες υποθέσεις, αποτελούν τροχοπέδη στην υιοθέτηση του Civitas στον πραγματικό κόσμο. Η λύση που δόθηκε στο [24] (και περιγράφετε στην παρούσα διπλωματική εργασία στην αναφορά για την φάση προετοιμασίας και ρύθμισης)φαίνεται να έγινε αποδεκτή, και να υιοθετήθηκε σε επόμενες προτάσεις. Αυτό όχι μόνο επειδή βοηθά το σύστημα να προσπεράσει τις συγκεκριμένες υποθέσεις,αλλά και επειδή δίνει λύση σε ένα πρόβλημα που δεν είχε εντοπιστεί στην πρώτη έκδοση του Civitas, και αφορά σενάρια κατά τα οποία ο επιτιθέμενος συνεργαζόμενος με κάποιο από τους υπεύθυνους εγγραφών, έχει την δυνατότητα να αναγκάσει τον ψηφοφόρο να μην ψηφίσει καθόλου.

Βλέπουμε όμως πως η λύση που προτείνεται αναγκάζει τον ψηφοφόρο να πραγματοποιήσει την μισή εγγραφή όχι εξ αποστάσεως. Δημιουργήθηκε λοιπόν στον γράφοντα η εξής απορία:

Εφόσον σε μια ρεαλιστική και πρακτική υλοποίηση του συστήματος ένα μέρος της εγγραφής του χρήστη δεν γίνεται εξ αποστάσεως , γιατί να μην τύχει αυτό το γεγονός εκμετάλλευσης, ώστε να γίνουν κάποια πράγματα πιο απλά. Με αυτή την σκέψη, και σε συνδυασμό με το γεγονός ότι δεν θεωρώ ιδανική λύση οποιαδήποτε περιλαμβάνει υποθέσεις εμπιστοσύνης προς ανθρώπους , καταλήγω στην εξής διαδικασία εγγραφής:

α) Σε κάθε κέντρο στο οποίο θα γίνονται εγγραφές, θα υπάρχει ένα άτομο από κάθε πολιτική παράταξη
β) Προσερχόμενος ένας ψηφοφόρος στο κέντρο εγγραφής, εξετάζεται και πιστοποιείται η ταυτότητα του, και ότι όντως δικαιούται να εγγραφεί.
γ) Ο ψηφοφόρος παραδίδει προσωρινά στο άτομα των πολιτικών παρατάξεων οποιαδήποτε συσκευή είναι ικανή να τραβήξει φωτογραφίες ή/και βίντεο.
δ) Ο ψηφοφόρος εισέρχεται μόνος σε δωμάτιο το οποίο περιέχει έναν υπολογιστή.
ε) Τα άτομα των πολιτικών παρατάξεων δίνουν εντολή στον υπολογιστή στο δωμάτιο, να ετοιμαστεί να καταχωρήσει συνθηματικό για τον συγκεκριμένο υποψήφιο.
ζ) Ο υποψήφιος καταχωρεί το συνθηματικό και το δευτερεύον συνθηματικό (η λειτουργία του δευτερεύον συνθηματικού θα εξηγηθεί στην φάση ψηφοφορίας). Ταυτόχρονα ο υπολογιστής έξω από το δωμάτιο στον οποίο βρίσκονται τα άτομα των πολιτικών παρατάξεων , δεν τους δίνει την δυνατότητα να δουν το συνθηματικό που καταχώρησε ο ψηφοφόρος.
η) Το συνθηματικό κρυπτογραφείται και καταχωρείτε στην βάση του συστήματος.
θ) Εξ αποστάσεως ο ψηφοφόρος φροντίζει να εξασφαλίσει το δημόσιο συνθηματικό του.

Η πιο πάνω διαδικασία εκτελείται μια φορά για κάθε ψηφοφόρο , και το συνθηματικό μπορεί να ισχύει για κάθε εκλογική αναμέτρηση στην οποία δικαιούται να ψηφίσει ο χρήστης.

Οι στόχοι που προσπαθεί να ικανοποιήσει η πιο πάνω διαδικασία εγγραφής είναι η εξής:
α) Ο μόνος που γνωρίζει το ιδιωτικό συνθηματικό είναι ο ψηφοφόρος
β) Ο ψηφοφόρος δεν μπορεί να αποδείξει ότι το ιδιωτικό συνθηματικό είναι κάποιο συγκεκριμένο
γ) Η μυστικότητα του ιδιωτικού κλειδιού και άρα η επιτυχία ή όχι της άμυνας έναντι του εξαναγκασμού, δεν πρέπει να εξαρτάται από την εμπιστοσύνη του ψηφοφόρου σε οποιοδήποτε άτομο.
δ) Να διατηρείται η δυνατότητα αντιμετώπισης του εξαναγκασμού κατά τα πρότυπα του JCJ/Civitas.

Πως εξασφαλίζεται κάθε ένα από τα πιο πάνω σημεία:

α) Ο μόνος που θα βρίσκεται στο δωμάτιο με τον υπολογιστή είναι ο ψηφοφόρος. Ο υπολογιστής που βρίσκεται έξω από το δωμάτιο δεν παρέχει οποιαδήποτε πληροφορία για το τι καταχωρείται στον υπολογιστή μέσα στο δωμάτιο. Επιπλέον μόλις καταχωρήσει ο χρήστης το ιδιωτικό συνθηματικό , κρυπτογραφείται και αποθηκεύεται στην βάση δεδομένων του συστήματος. Φροντίζεται επίσης ότι ο υπολογιστής που θα τοποθετηθεί στο συγκεκριμένο δωμάτιο είναι απαλλαγμένος από κακόβουλα λογισμικά.

β) Ο υπολογιστής δεν εξάγει καμία ένδειξη που να υποδεικνύει το συνθηματικό που καταχώρησε ο ψηφοφόρος (receipt free). Επιπλέον απαγορεύεται να μπει ο χρήστης στο δωμάτιο με οποιοδήποτε οπτικο-ακουστικό υλικό ώστε να μην είναι σε θέση να καταγράψει το τι εισήγαγε στον υπολογιστή, και να χρησιμοποιήσει την καταγραφή ως μέσω απόδειξης .

γ)Όπως ειπώθηκε ο ψηφοφόρος μπαίνει στο δωμάτιο μόνος του. Επιπλέον τα άτομα που βρίσκονται και επιβλέπουν στον εξωτερικό χώρο είναι ένας από κάθε πολιτική παράταξη, και άρα υπό την ύπαρξη αντικρουόμενων συμφερόντων , κανένας δεν θα προσπαθήσει να επηρεάσει τον χρήστη. Αν υπήρχε μόνο ένα άτομο, τότε θα υπήρχε το ενδεχόμενο αυτός να συνεργάζεται με τον επιτιθέμενο και να μπει στο δωμάτιο με τον χρήστη , απαιτώντας από αυτόν δει την καταχώρηση του συνθηματικού .

δ) Έχοντας το ιδιωτικό συνθηματικό ο χρήστης ,τότε σε περίπτωση που είναι θύμα εξαναγκασμού, μπορεί να συμπεριφερθεί με ακριβώς τον ίδιο τρόπο που συμπεριφέρεται ένας ψηφοφόρος του συστήματος Civitas. Το πλεονέκτημα , είναι το γεγονός ότι επειδή τα συνθηματικά δεν παράγονται με κάποιο τρόπο, αλλά επιλέγονται κατά προτίμησή του χρήστη , το ίδιο εύκολα μπορεί ο χρήστης να αποφασίσει ένα ψεύτικο συνθηματικό και να ενημερώσει τον επιτιθέμενο για το συγκεκριμένο . Το σύστημα , θα συμπεριφέρεται με τον ίδιο τρόπο στον ψηφοφόρο, είτε το συνθηματικό είναι αληθής είτε το συνθηματικό είναι ψευδές, ώστε να μην μπορεί ο επιτιθέμενος να ξεχωρίσει τις περιπτώσεις. Λόγο του γεγονότος ότι και τα δύο συνθηματικά αληθές/ψευδές , είναι επιλογές του χρήστη, δεν υπάρχει περίπτωση ο επιτιθέμενος να είναι σε θέση να ξεχωρίσει το αληθές από το ψευδές.

Κεφάλαιο 5

Παρουσίαση συστήματος ηλεκτρονικής ψηφοφορίας – CyVotingSystem

Η διαδικτυακή εφαρμογή που υλοποιεί σύστημα ψηφοφορίας, ανθεκτικό στον εξαναγκασμό είναι υλοποιημένη σε γλώσσα python , χρησιμοποιώντας το framwork Django. Επιπλέον έγεινε χρήση twitter Bootstrap για CSS , έτσι ώστε να ρυθμίζεται εύκολα η επιθυμητή εμφάνιση της σελίδας σε κάθε μέγεθος οθόνης.

Το Django είναι ένα “πλαίσιο” προγραμματισμού , μέσω του οποίου είναι δυνατή η δημιοργεία εφαρμογών ιστού. Με την χρήση της γλώσσας python, δηλαδή εφαρμογές που θα τρέχουν σε εξυπηρετητή και θα παράγουν δυναμικά περιεχόμενο html , css και πάντα ανάλογα με τις αιτήσεις που δέχεται από τους χρήστες. Ο αναγνώστης μπορεί να μάθει περισσότερα για το Django: https://www.djangoproject.com/

Ένα πρόβλημα που μπορεί να προκύψει με τις εφαρμογές ιστού, είναι πως μπορεί να θέλουμε για διαφορετικά μεγέθοι οθονών (κινητά, ταμπλέτες, προσωπικούς υπολογιστές), να εμφανίζουμε περιεχόμενο με διαφορετικό τρόπο. Με την χρήση του twitter bootstrap ο προγραμματιστής έχει την ευκαιρία να πάρει έτοιμα πρότυπα και να τα τροποποιήσει στις δικές του απαιτήσεις, ώστε η εφαρμογή ιστού να παρουσιάζεται όπως θέλει σε όποιοδίποτε μέγεθος οθόνης. Ο αναγνώστης μπορεί να μάθει περισσότερα για το twitter boostrap: http://getbootstrap.com/

5.1 Απαιτήσεις χρήστη

Το ηλεκτρονικό σύστημα εκλογών που παρουσιάζεται παρέχει δυνατότητα πρόσβασης μόνο στους εγγεγραμμένους ψηφοφόρους για την συγκεκριμένη ψηφοφορία.

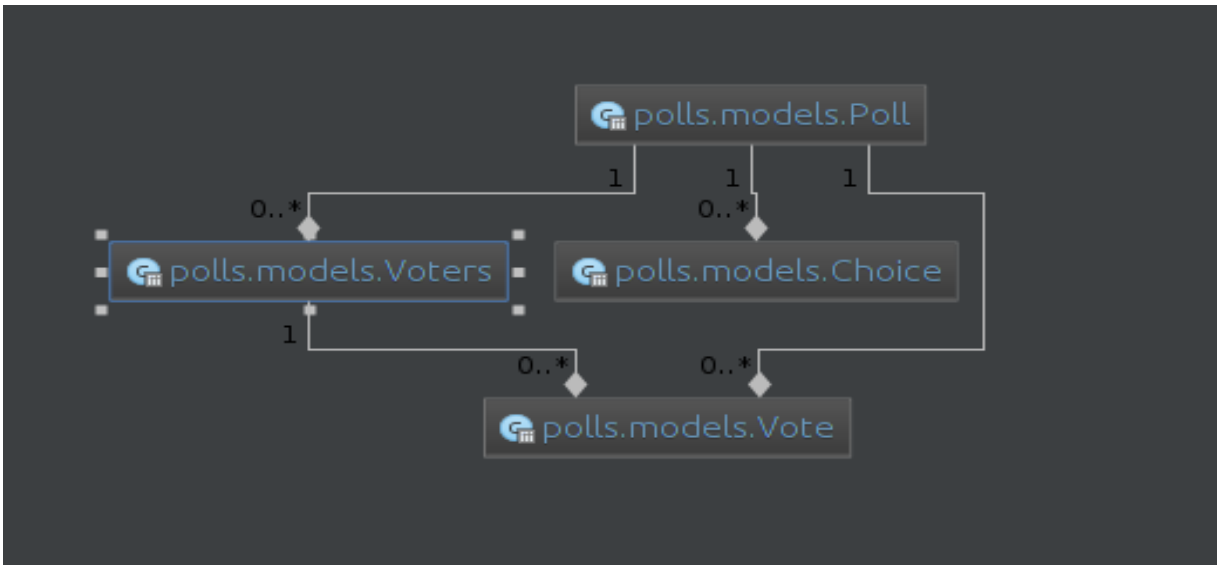
Είναι σε θέση να ενσωματώσει την βάση δεδομένων με τους εγγεγραμμένους χρήστες μαζί με τα κρυπτογραφημένα συνθηματικά τους . Μπορεί να χειριστεί την διαδικασία δημιουργίας εκλογών

παράγοντας από αυτή την διαδικασία ένα μοναδικό αριθμό ο οποίος αντιστοιχεί στην εκλογική διαδικασία η οποία μόλις δημιουργήθηκε . Επιπλέον είναι σε θέση να χειριστεί την διαδικασία της ψηφοφορίας μετρώντας ως έγκυρη ψήφο αυτή με το σωστό συνθηματικό και αν ένας χρήστης ψηφίσει μόνο μια φορά μετρά ως έγκυρη η πρώτη.

5.2 Λειτουργία συστήματος

Για την επεξήγηση της λειτουργίας του συστήματος, χρειάζεται η παρουσίαση του σχήματος της βάσης δεδομένων που δημιουργήθηκε για να κρατά τα δεδομένα που χρειάζεται το σύστημα για να λειτουργήσει . Για τους σκοπούς αυτής της υλοποίησης χρησιμοποιήθηκε sqlite3 .

Διάγραμμα :



Εικόνα 5.1 ERD δεδομένων του συστήματος

```
BEGIN;
CREATE TABLE "polls_poll" (
    "id" integer NOT NULL PRIMARY KEY,
    "question" varchar(200) NOT NULL,
    "pub_date" datetime NOT NULL,
    "end_date" datetime NOT NULL
)
;
CREATE TABLE "polls_choice" (
    "id" integer NOT NULL PRIMARY KEY,
    "poll_id" integer NOT NULL REFERENCES "polls_poll" ("id"),
    "choice_text" varchar(200) NOT NULL,
    "votes" integer NOT NULL
)
;
CREATE TABLE "polls_voters" (
    "id" integer NOT NULL PRIMARY KEY,
    "election_id_id" integer NOT NULL REFERENCES "polls_poll" ("id"),
    "voter_id" integer NOT NULL,
    "hash_value" varchar(200) NOT NULL,
    "correct_vote" varchar(200) NOT NULL
)
;
CREATE TABLE "polls_vote" (
    "id" integer NOT NULL PRIMARY KEY,
    "Voter_id_id" integer NOT NULL REFERENCES "polls_voters" ("id"),
    "choice_id" varchar(200) NOT NULL,
    "election_id_id" integer NOT NULL REFERENCES "polls_poll" ("id")
)
;
CREATE INDEX "polls_choice_763e883" ON "polls_choice" ("poll_id");
CREATE INDEX "polls_voters_9f7e01b0" ON "polls_voters" ("election_id_id");
CREATE INDEX "polls_vote_bd67129a" ON "polls_vote" ("Voter_id_id");
CREATE INDEX "polls_vote_9f7e01b0" ON "polls_vote" ("election_id_id");
COMMIT;
```

Εικόνα 5.2 Κώδικας για την δημιουργεία της βάσης στο 5.1

User Interfaces

Χρησιμοποιώντας την γραφική διεπαφή ο χρήστης μπορεί να :

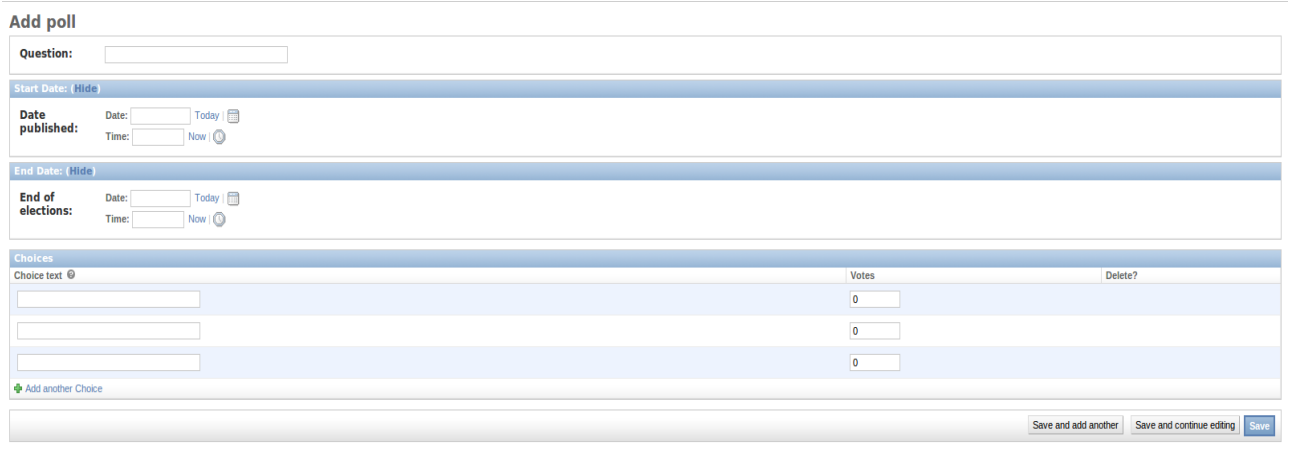
- Καταχωρήσει την μοναδικό αριθμό της εκλογικής αναμέτρησης για να ψηφίσει
- Επικοινωνήσει με τους υπεύθυνους του συστήματος
- Έχει πρόσβαση στον κώδικα του συστήματος

5.2.1 Δημιουργεία εκλογών

Ο υπεύθυνος εκλογών επικοινωνεί με τον υπεύθυνο του συστήματος μέσω φόρμας επικοινωνίας που υπάρχει στην σελίδα του συστήματος, και αιτείται την δημιουργία εκλογικής διαδικασίας μέσω του συστήματος. Ο υπεύθυνος εκλογών παρέχει τα εξής:

- Τύπος/Όνομα εκλογικής διαδικασίας
- Ημερομηνία/'Ωρα έναρξης
- Ημερομηνία / Ώρα λήξης
- Σχεδιασμός ψηφοδελτίου
- Υποψήφιοι
- Εκλογικός κατάλογος αυτών που δικαιούνται να συμμετάσχουν, μαζί με τα κρυπτογραφημένα ιδιωτικά κλειδιά των ψηφοφόρων

  Ο υπεύθυνος του συστήματος δημιουργεί νέες εκλογές συμπληρώνοντας την κατάλληλη φόρμα:



Εικόνα 5.3 Κώδικας για δημιουργεία εκλογών

Δημιουργώντας ο υπεύθυνος του συστήματος την εκλογική διαδικασία, ενσωματώνει σε αυτή την βάση με τους εγκεκριμένους ψηφοφόρους και τα ιδιωτικά τους κλειδιά. Ακολούθως γνωστοποιεί στον υπεύθυνο εκλογών τον μοναδικό αριθμό της εκλογικής διαδικασίας , και αυτός με την σειρά του έχει ευθύνη να το γνωστοποιήσει σε όσους θα συμμετάσχουν στις εκλογές.

Σημειώνεται επίσης, ότι κανένας δεν θα είναι σε θέση να καταχωρήσει ψήφο πριν την ημερομηνία και ώρα έναρξης, ενώ κατά την ημερομηνία και ώρα λήξης οι κάλπες κλείνουν .

5.2.2 Φάση εγγραφής

Η φάση της εγγραφής όπως εξηγήθηκε σε προηγούμενη ενότητα, αποφασίστηκε ότι δεν θα γίνεται εξ αποστάσεως, ώστε να επιτευχθεί ευκολότερα ο στόχος δημιουργίας ιδιωτικού συνθηματικού.
Συγκεκριμένα η διαδικασία έχει ως εξής:
α) Σε κάθε κέντρο στο οποίο θα γίνονται εγγραφές, θα υπάρχει ένα άτομο από κάθε πολιτική παράταξη
β) Προσερχόμενος ένας ψηφοφόρος στο κέντρο εγγραφής, εξετάζεται και πιστοποιείται η ταυτότητα του, και ότι όντως δικαιούται να εγγραφεί.
γ) Ο ψηφοφόρος παραδίδει προσωρινά στο άτομα των πολιτικών παρατάξεων οποιαδήποτε συσκευή είναι ικανή να τραβήξει φωτογραφίες ή/και βίντεο.
δ) Ο ψηφοφόρος εισέρχεται μόνος σε δωμάτιο το οποίο περιέχει έναν υπολογιστή.
ε) Τα άτομα των πολιτικών παρατάξεων δίνουν εντολή στον υπολογιστή στο δωμάτιο, να ετοιμαστεί να καταχωρήσει συνθηματικό για τον συγκεκριμένο ψηφοφόρο.
ζ) Ο ψηφοφόρος καταχωρεί το συνθηματικό και το δευτερεύον συνθηματικό (η λειτουργία του δευτερεύον συνθηματικού θα εξηγηθεί στην φάση ψηφοφορίας). Ταυτόχρονα ο υπολογιστής έξω από το δωμάτιο στον οποίο βρίσκονται τα άτομα των πολιτικών παρατάξεων , δεν τους δίνει την δυνατότητα να δουν το συνθηματικό που καταχώρησε ο ψηφοφόρος.
η) Το συνθηματικό κρυπτογραφείται και καταχωρείτε στην βάση του συστήματος.
θ) Εξ αποστάσεως ο ψηφοφόρος φροντίζει να εξασφαλίσει το δημόσιο συνθηματικό του.

Το αρχείο στο οποίο καταχωρούνται τα στοιχεία εγγραφής των ψηφοφόρων κρυπτογραφείται με συμμετρική κρυπτογραφία, και αποκρυπτογραφείται για ανανέωση κάθε φορά που θα υπάρχει ανάγκη για εγγραφή νέων ψηφοφόρων. Κατά την δημιουργία νέας εκλογικής διαδικασίας τα αρχεία/ κατάλογοι ψηφοφόρων αποστέλλονται κρυπτογραφημένα στους υπεύθυνους του συστήματος εκλογών . Το σύστημα φροντίζει να αποκρυπτογραφήσει το συγκεκριμένο αρχείο και να ενσωματώσει στην βάση του τα περιεχόμενα του.

Ο λόγος που κρυπτογραφείται το αρχείο είναι σε περίπτωση που κλαπεί , να μην γίνει γνωστό ποιοι ψηφίσαν.

Κώδικας για την εγγραφή χρηστών

population_script_1.py

```
#__author__ = 'gkoume01'
#__date__='17-4-2014'
import hashlib
import getpass

id=0
password=0
f = open('voters.txt', 'w')
while True:
        id=raw_input('Type your ID number: ')
        # id=sys.stdin.read()
        if id=='stop':
            break
        print 'Type your password: '
        pw = getpass.getpass()
        h=hashlib.sha256(pw).hexdigest()
        correct_vote=raw_input('Value for correct vote: ')
        line=id+"\t"+h+'\t'+correct_vote+'\n'
        f.write(line)
f.close()
```

Εικόνα 5.3 Κώδικας για την εγγραφή χρηστών. population_script_1.py

Ενσωμάτωση των εγγεγραμμένων ψηφοφόρων στο σύστημα (πιθανότατα να είναι διαφορετικό σύνολο ψηφοφόρων για κάθε εκλογική αναμέτρηση)

```
__author__ = 'gkoume01'
import os
election_id=3 ######Change for each election-SOS

def populate():
    f = open('voters.txt')
    lines = f.readlines()
    f.close()
    i=0
    while i<lines.__len__():
     #print lines[i]
        splits1=lines[i].split("\t",3)
        id=int(splits1[0])
        hash=splits1[1]
        cv=splits1[2]

        Voters.objects.get_or_create(voter_id=id,hash_value=hash,election_id=election_id,correct_vote=cv)

# Start execution here!
if __name__ == '__main__':
    print "Starting population script..."
    os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'pollsite.settings')
    from polls.models import Voters
    populate()
```

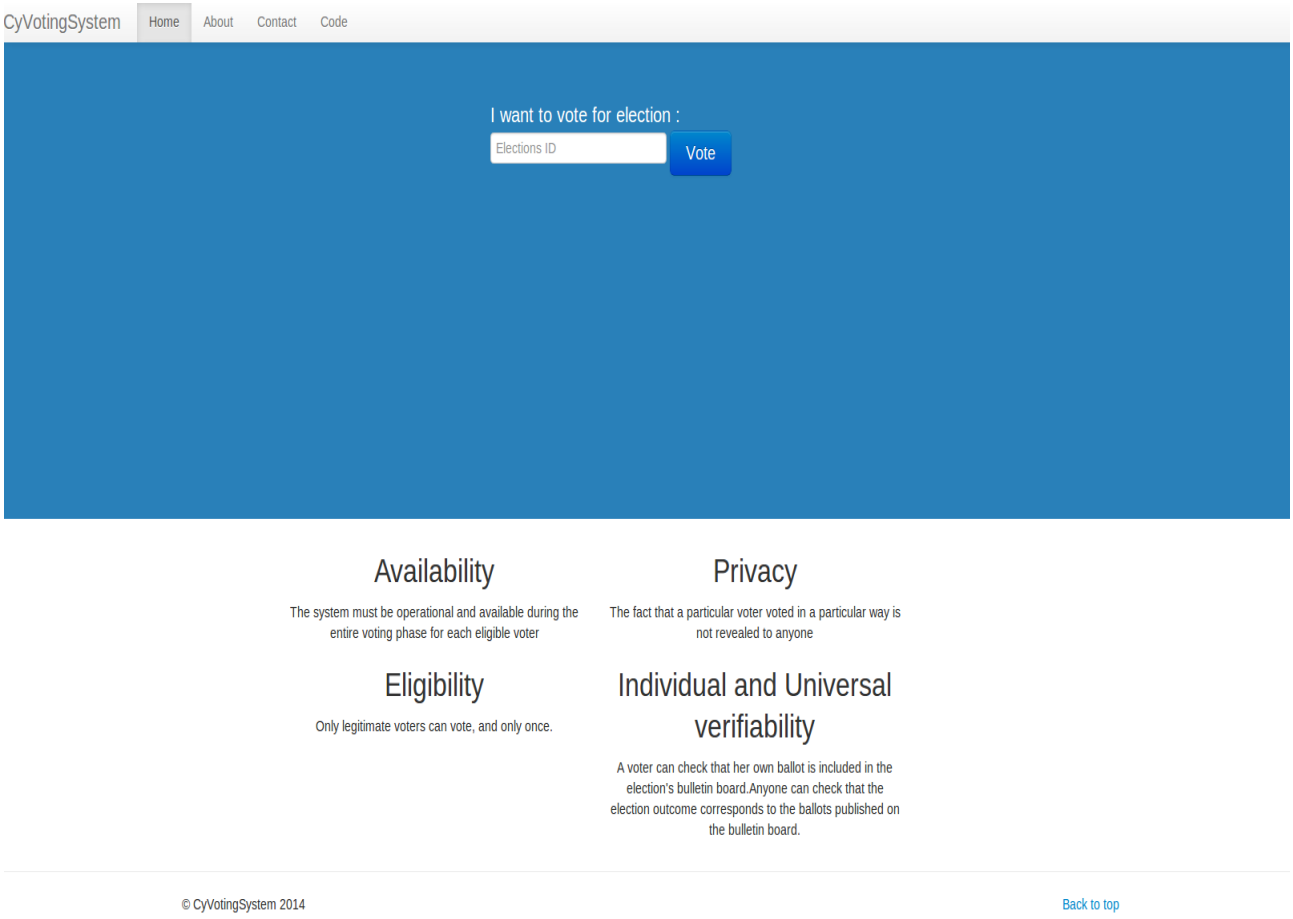
Εικόνα 5.4 Κώδικας για την ενσωμάτοση ψηφοφόρων στο σύστημα. population_script_2.py

Με τα στοιχεία των ψηφοφόρων στην βάση δεδομένων του συστήματος το σύστημα μπορεί να ελέγχει αν ένας χρήστης δικαιούται να ψηφίσει σε μια εκλογική αναμέτρηση.

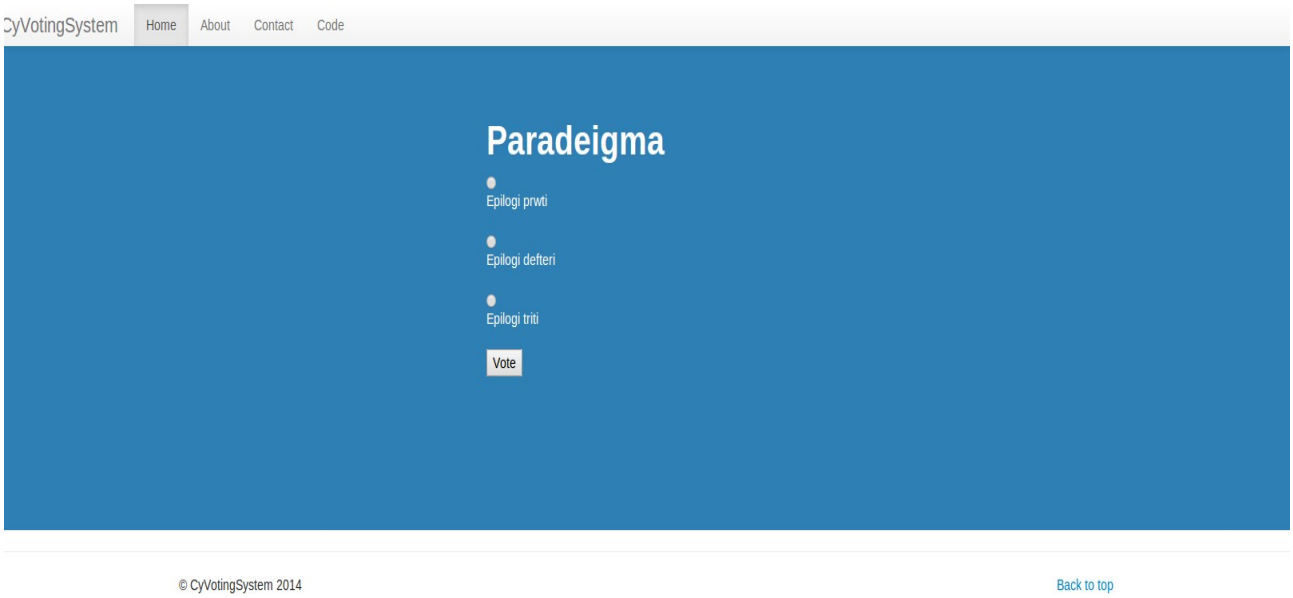
5.2.3 Φάση ψηφοφορίας

Από την έναρξη των εκλογών και μετά , οι χρήστες μπορούν να επισκέπτονται την ιστοσελίδα των εκλογών για να ψηφίσουν.

Ο χρήστης καταχωρεί στο πεδίο κειμένου το μοναδικό αριθμό της εκλογικής διαδικασίας στην οποία θέλει να συμμετάσχει και επιλέγει “Vote”. Ακολούθως παραπέμπεται στο ψηφοδέλτιο , και έχει την δυνατότητα να επιλέξει τον υποψήφιο (ή την απάντηση αν πρόκειται για δημοψήφισμα) , της αρεσκείας του. Μέχρι αυτό το σημείο μπορεί ο κάθε χρήστης να φτάσει, είτε δικαιούται είτε δεν δικαιούται να ψηφίσει.

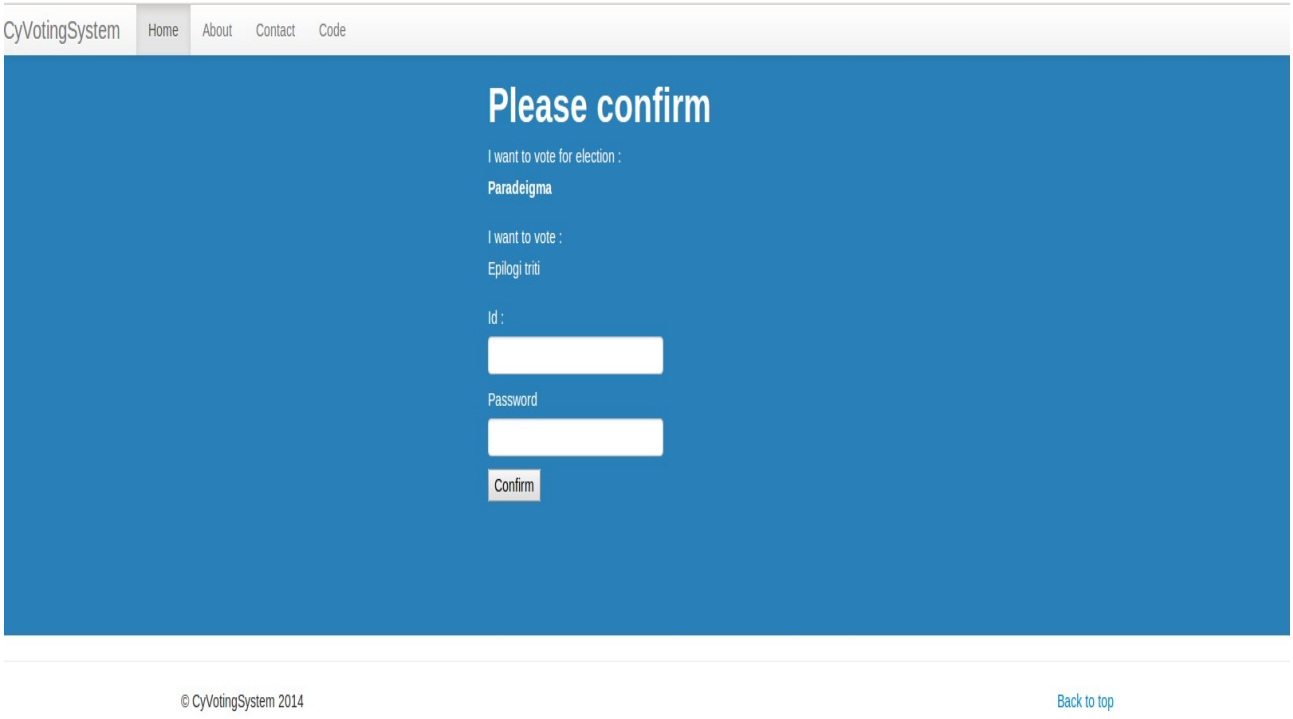


Εικόνα 5.5 Κεντρική σελίδα του συστήματος.



Εικόνα 5.4 Ο χρήστης μπορεί να επιλέξει την απάντηση που θέλει

Επιλέγοντας ο χρήστης , και πατώντας στο “vote”, παραπέμπεται σε σελίδα όπου χρειάζεται να καταχωρήσει τον αριθμό της ταυτότητας του και το ιδιωτικό του κλειδί, έτσι ώστε να ελεγχθεί καταρχάς αν δικαιούται να ψηφίσει, και επιπλέον ελέγχοντας το συνθηματικό που καταχώρησε, αποφασίζεται αν η ψήφος θα ληφθεί υπόψιν ή όχι.



Εικόνα 5.4 Έλεγχος αν ο χρήστης δικαιούται να ψηφίσει στην συγκεκριμένη ψηφοφορία

Σε κάθε περίπτωση, είτε αποφασιστεί πως θα ληφθεί υπόψιν , είτε όχι, εμφανίζεται μήνυμα που ενημερώνει τον χρήστη για την ψήφο του, και τον ευχαριστεί. Αν η ψήφος θα ληφθεί υπόψιν δίπλα από την ψήφο θα παρουσιαστεί το δευτερεύον συνθηματικό του χρήστη, ως ένδειξη από το σύστημα ότι αναγνωρίζει πως η ψήφος αυτή πρέπει να μετρήσει. Σε αντίθετη περίπτωση παρουσιάζονται 5 τυχαίοι χαρακτήρες.

Όταν η εκλογική διαδικασία τελειώσει και τα αποτελέσματα είναι έτοιμα, τότε όποισδήποτε καταχωρήσει τον μοναδικό αριθμό της εκλογικής αναμέτρησης που έληξε, παραπέμπεται σε σελίδα που παρουσιάζει τα αποτελέσματα.

Στον σύστημα ψηφοφορίας που παρουσιάστηκε δόθηκε έμφαση στην αντιμετώπιση του προβλήματος εξαναγκασμού, αλλάζοντας την διαδικασία εγγραφής , και **δεν** παρέχεται επαλήθευση των αποτελεσμάτων.

Κεφάλαιο 6

Συμπεράσματα

Όπως ανέφερα κατά την εισαγωγή, η ψηφοφορίες μέσω διαδικτύου μπορούν να δώσουν την ευκαιρία για ένα ισχυρότερο δημοκρατικό πολίτευμα, όπου το κόστος διεξαγωγής δημοψηφισμάτων δεν θα είναι αιτία για να μην μπορεί να εκφράζεται ο λαός. Τέθηκε το εξής ερώτημα κατά την εισαγωγή:

“Αφού μπορώ να εμπιστευτώ τις συναλλαγές , και τα χρήματα μου στο διαδίκτυο, γιατί να μην μπορώ να εμπιστευτώ την ψήφο μου;”

Πέρα από τις υπάρχουσες επιθέσεις σε διαδικτυακές εφαρμογές, και οι οποίες δεν αφορούν αποκλειστικά συστήματα ψηφοφορίας, αλλά είναι γενικότερες, έγινε προσπάθεια να παρουσιαστούν κάποια από τα βασικά προβλήματα που εμποδίζουν την υιοθέτηση συστημάτων διαδικτυακής ψηφοφορίας σε πραγματικές εκλογές.

Το Civitas είναι ένα σύστημα που έφερε τις ψηφοφορίες μέσω διαδικτύου ένα βήμα πιο κοντά στην πραγματικότητα καλύπτοντας τις απαιτήσεις επαληθευσιμότητας των αποτελεσμάτων και αντίστασης στον εξαναγκασμό. Στην συγκεκριμένη διπλωματική εργασία παρουσιάστηκαν κάποιες από τις υποθέσεις εμπιστοσύνης που κάνει το σύστημα , και αναλύθηκαν περισσότερο αυτές που αφορούν την διαδικασία εγγραφής. Αυτές οι υποθέσεις εμπιστοσύνης είναι που κάνουν την χρήση του Civitas ανέφικτη για πραγματικές εκλογικές αναμετρήσεις. Έτσι σαν μελλοντική εργασία θεωρώ πως θα ήταν χρήσιμη η μελέτη των υποθέσεων που κάνει το Civitas ώστε να βρεθούν τρόποι να είναι πιο “χαλαρές” και όχι τόσο απαιτητικές, ώστε να είναι εφικτή η χρήση του Civitas υπό τις παρούσες συνθήκες. Για παράδειγμα παρουσιάστηκε πως η διαδικασία εγγραφής μπορεί να γίνεται μερικός εξ αποστάσεως ή εξ ολοκλήρου εξ αποστάσεως ώστε οι 2 πρώτες υποθέσεις που αφορούν την διαδικασία εγγραφής και παραγωγής συνθηματικών να “χαλαρώσουν”. Αντίστοιχα πρέπει να μελετηθεί ποιες αλλαγές πρέπει να γίνουν στο σύστημα ώστε να αλλάξουν οι απαιτήσεις εμπιστοσύνης προς το καλύτερο.

Βιβλιογραφία

[1] David L. Dill, Bruce Schneier, and Barbara Simons. Voting and technology: Who gets to count your vote? Communications of the ACM, 46(8):29–31, Aug. 2003.

[2] David Evans and Nathanael Paul. Election security: Perception and reality. IEEE Security & Privacy, 2(1):24–31, Jan. 2004

[3]David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. Analyzing Internet voting security . Communications of the ACM, 47(10):59–64, Oct. 2004.

[4] Aviel D. Rubin. Security considerations for remote electronic voting. Communications of the ACM, 45(12):39–44, Dec. 2002

[5]The National Election Committee. E-voting system - overview. Technical report, The National Election Committee, Estonia 2005

[6] Fabian Breuer and Alexander H. Trechsel. E-voting in the 2005 local elections in estonia. Technical report, Council Of Europe, 2006.

[7] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In ACM Symposium on Theory of Computing (STOC), pages 544–553. ACM Press, May 1994.

[8] Martin Hirt. Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting. PhD thesis, ETH Zurich, September 2001.

[9]Krishna Sampigethaya and Radha Poovendran. A framework and taxonomy for comparison of electronic voting schemes. Computers Security, 25, issue 2:137–153, March 2006.

[10] Tatsuaki Okamoto. An electronic voting scheme. In IFIP World Conference on IT Tools, pages 21–30, 1996.

[11] Byoungcheon Lee and Kwangjo Kim. Receipt-free electronic voting through collaboration of voter and honest verifier. In Workshop on Information Security and Cryptology, 2000. Pages:101-108

[12] Emmanouil Magkos, Mike Burmester, and Vassilios Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In I3E 2001, volume 202 of IFIP Conference Proceedings, pages 683–694. Kluwer, 2001.

[13] Miroslaw Kutylowski and Filip Zagorski. Coercion-free internet voting with receipts. In Workshop on Electronic Voting and e-Government in the UK, Edinburgh, UK, February 2006.

[14]S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In ACM Symposium on Theory of Computing (STOC ’85), pages 291–304. ACM Press, 1985.

[15] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. SIAM Journal on Computing, 18(1):186–208, 1989.

[16] Oded Goldreich. Zero-knowledge twenty years after its invention, 2002.

[17]Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Advances in Cryptology - CRYPTO 86, volume 263 of Lecture Notes in Computer Science, pages 186–194. Springer-Verlag, August 1986.

[18] Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979

[19] Liu, C.L. Introduction to Combinatorial Mathematics. McGraw-Hill, New York, 1968.

[20] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–88, 1981.

[21]Stephanie Delaune, Sergiu Bursuc,Peter Y. A. Ryan Caveat Coercitor: coercion-evidence in electronic voting , 19-22 May 2013 IEEE Symposium on Security and Privacy . Page(s):367 - 381

[22] Stephan Neumann, Christian Feier , Melanie Volkamer,Reto E. Koenig Towards A Practical JCJ / Civitas Implementation . Book title: Informatik 2013 Informatik angepasst an Mensch, Organisation und Umwelt , Pages: 804-818 .

[23] Stephanie Delaune, Steve Kremer, Mark Ryan. Coercion-Resistance and Receipt-Freeness in Electronic Voting. Book title : Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06) . Pages : 28-39, publisher : IEEE Computer Society Press .

[24]Stephan Neumann και Melanie Volkamer ,Civitas and the Real World: Problems and Solutions from a Practical Point of View . Book title: 7th International Conference on Availability, Reliability and Security (ARES). Pages: 180-185

[25]Ralf Kusters και Tomasz Truderung. An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols. IEEE Symposium on Security and Privacy 2009: 251-266

[26] Fateme Shirazi , Stephan Neumann, Ines Ciolacu, Melanie Volkamer. Robust Electronic Voting : Introducing Robustness in Civitas. REVOTE, page 47-55. IEEE, (2011)

[27] Civitas: Toward a Secure Voting System .Security and Privacy, 2008. SP 2008. IEEE Symposium on. 354 - 368